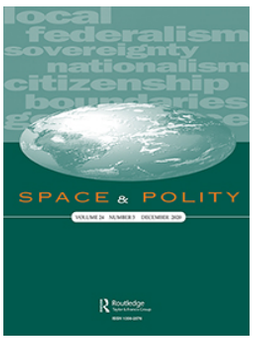

Space and Polity

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/cspp20

Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of COVID-19

Rob Kitchin

To cite this article: Rob Kitchin (2020) Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of COVID-19, Space and Polity, 24:3, 362-381, DOI: 10.1080/13562576.2020.1770587

To link to this article: https://doi.org/10.1080/13562576.2020.1770587

Published online: 03 Jun 2020.

SPACE AND POLITY
2020, VOL. 24, NO. 3, 362–381
https://doi.org/10.1080/13562576.2020.1770587

Civil liberties *or* public health, or civil liberties *and* public health? Using surveillance technologies to tackle the spread of COVID-19

Rob Kitchin

Department of Geography and Maynooth University Social Sciences Institute, Maynooth University, County Kildare, Ireland

ABSTRACT

To help tackle the spread of COVID-19 a range of surveillance technologies – smartphone apps, facial recognition and thermal cameras, biometric wearables, smart helmets, drones, and predictive analytics – have been rapidly developed and deployed. Used for contact tracing, quarantine enforcement, travel permission, social distancing/movement monitoring, and symptom tracking, their rushed rollout has been justified by the argument that they are vital to suppressing the virus, and civil liberties have to be sacrificed for public health. I challenge these contentions, questioning the technical and practical efficacy of surveillance technologies, and examining their implications for civil liberties, governmentality, surveillance capitalism, and public health.

ARTICLE HISTORY
Received 2 May 2020
Accepted 13 May 2020

KEYWORDS
COVID-19; surveillance; civil liberties; governmentality

Introduction

As the COVID-19 pandemic has swept the world it has been accompanied by strategies and tactics designed to combat and mitigate its effects. In the main, a traditional public health approach has been pursued involving phases of containment (steps to prevent the virus from spreading), delay (measures to reduce the peak of impact), mitigation (providing the health system with necessary supports) and research (seeking additional effective measures and a cure). Typical measures employed in the delay and containment phases have involved increased and more vigorous personal hygiene, wearing protective clothing, practicing social distancing and self-isolation, banning social gatherings, limiting travel, enforced quarantining and lockdowns, and testing regimes.

Existing and new digital technologies are being harnessed to augment and supplement these traditional measures, accompanied by arguments that they will improve their effectiveness through real-time mass monitoring at the individual and aggregate level, in turn optimizing population control. Indeed, a number of states were relatively quick to deploy

CONTACT Rob Kitchin rob.kitchin@mu.ie MUSSI, Iontas Building, North Campus, Maynooth University, Maynooth, County Kildare, Ireland

This paper was written in April 2020 during a quickly unfolding event as technologies were being created, repurposed and deployed, and prior to any detailed, systematic empirical assessment of the technical or ethical aspects having been undertaken. It therefore needs to be read with that framing in mind.

technology-led solutions to aid their response to the conoravirus for five primary purposes: (1) quarantine enforcement/travel permission (knowing people are where they should be, either enforcing home isolation for those infected or close contacts, or enabling approved movement for those not infected); (2) contact tracing (knowing whose path people have crossed); (3) pattern and flow modelling (knowing the distribution of the disease and its spread and how many people passed through places); (4) social distancing and movement monitoring (knowing if people are adhering to recommended safe distances and to circulation restrictions); and (5) symptom tracking (knowing whether the population are experiencing any symptoms of the disease) (The Economist, 2020). In addition, states and supra-states (e.g. European Union) have actively promoted the rapid prototyping and development of new tech solutions through funded research and enterprise programmes[1] and sponsoring hackathons.[2]

With respect to quarantine enforcement/travel permissions, citizens in some parts of China are required to install an app on their phone and then scan QR codes when accessing public spaces (e.g. shopping malls, office buildings, communal residences, metro systems) to verify their infection status and permission to enter, alerting local police if they should be in quarantine (Goh, 2020). Moscow authorities have rolled out an app system to pre-approve journeys and routes, and enforce quarantining; registration requires a person to link their smartphone to the city's e-gov system, and upload personal IDs, employer tax identifier and vehicle number plate (Ilyushina, 2020). Taiwan has deployed a mandatory phone-location tracking system to enforce quarantines (issuing GPS-enabled[3] phones to those that do not own one), sending text messages to those who stray beyond their lockdown range and issuing fines for violations (Timberg & Harwell, 2020). The Polish government has introduced a home quarantine app that requires people in isolation to take a geo-located selfie of themselves within 20 minutes of receiving an SMS or risk a visit from the police (Nielsen, 2020). Hong Kong has issued electronic tracker wristbands to ensure compulsory home quarantine is observed (Stanley & Granick, 2020).

Israel repurposed its advanced digital monitoring tools normally used for counterterrorism to track the movement of phones owned by coronavirus carriers in the 14 days prior to testing positive in order to trace close contacts (Cahane, 2020).[4] In South Korea, the government is utilizing surveillance camera footage, smartphone location data, and credit card purchase records to track positive cases and their contacts (Singer & Sang-Hun, 2020). Singapore quickly launched TraceTogether, a bluetooth enabled app that detects and stores the details of nearby phones to enable contact tracing (Singer & Sang-Hun, 2020). As of mid-April, 28 countries had produced contact tracing apps with another 11 planning to launch imminently (Linklaters, 2020).[5] In the US, airline companies were instructed to communicate the name and contact information of all passengers and crew arriving in the country within 24 hours to the Center for Disease Control (Guarglia & Schwartz, 2020).

Other states have utilized technologies designed to measure biometric information. For example, hand-held thermal cameras have been used in a number of countries to screen movement in public space and by companies to screen access to workspaces (Nellis, 2020). Italy has been using thermal cameras mounted on drones to monitor the temperature of people in public space, as well as to police the breaking of lockdown restrictions (Url, 2020). Police in the United Arab Emirates are using 'smart helmets' to scan up to 200

peoples' body temperature a minute (Reuters, 2020). Liechtenstein is piloting the use of biometric bracelets to monitor in real-time vital bodily metrics including skin temperature, breathing and heart rate of wearers, with the aim to deploy across all citizens within months (Jones, 2020).

A number of companies have offered, or have actively undertaken, to repurpose their platforms and data as a means to help tackle the virus. Most notably, Apple and Google, who provide operating systems for iOS and Android smartphones, are developing solutions to aid contact tracing (Brandom & Robertson, 2020), with Google also monitoring the effects of interventionist measures across cities and regions globally.[6] In Germany, Deutsche Telekom are providing aggregated, anonymized information to the government on people's movements; likewise Telecom Italia, Vodafone and WindTre are doing the same in Italy (Pollina & Busvine, 2020). NSO Group, the company behind Israel's contact tracing solution, have offered their services to a number of governments (Martin, 2020), as have other cyber-intelligence companies such as Cellebrite, Intellexa, Verint Systems, Rayzone Group, Cobwebs Technologies and Patternz (Schectman et al., 2020). Unacast, a location-based data broker, is using GPS data harvested from apps installed on smartphones to determine if social distancing is taking place (Fowler, 2020), creating a social distancing scorecard for every county in the United States, and partnering with individual states to help determine if implemented measures are working (Hoonhout, 2020).

Palantir, a secretive data analytics company with a reputation for working with police and intelligence agencies (McDonald, 2020; Sadowski, 2020), is monitoring and modelling the spread of the disease to predict the required health service response for the Center for Disease Control in the US and the National Health Service in the UK, and has pitched its services to other states (Hatmaker, 2020). In the US, Clearview AI has pitched using its facial recognition services on CCTV footage to identify people who are in close contact with each other in public and private spaces (NBC News, 2020), and in the UK, Onfido have offered to link testing results with facial recognition to create 'immunity passports' to regulate movement (Proctor & Devlin, 2020). Experian, a large global data broker and credit scoring company, has announced it will be combing through its 300 million consumer profiles to identify those likely to be most impacted by the pandemic and offering the information to 'essential organizations', including health care providers, federal agencies and NGOs (Wodinsky, 2020). Facebook, and smaller location tracking companies Cuebiq and Camber Systems, are sharing movement data with infectious disease researchers to monitor social distancing across the US (Paul et al., 2020). A Twitter thread by Wolfie Christl provides a list of other location tracking companies offering coronavirus analytics or data to government and researchers for tackling the pandemic, including Foursquare, SafeGraph, Placer, Umlaut, Gravy Analytics, and PlaceIQ.[7]

Many politicians, policy makers and citizens might believe that surveillance technologies are legitimately deployed if they help to limit the spread of the virus and thereby save lives, regardless of any concerns with respect to privacy or governmentality. Indeed, those who promote their use argue that the requirements of public health trump any concerns over civil liberties. But is it only possible to have public health *or* civil liberties, or is that a false trade-off? Or is it even a false trade, given that the validity and effectiveness of these technologies is not yet proven? Are we rushing into invasive

surveillance with immediate and downstream consequences concerning civil liberties, citizenship and surveillance capitalism with little benefit in return? These questions deserve careful consideration and in this paper I provide initial answers and outline an agenda for documenting how these technologies unfold in practice and impact on governmentality and the wider political economy (see Table 1 for a summary of issues).

Will technology solutions be effective?

At the time of writing (April 2020), potential digital solutions to the spread of COVID-19 are being rushed into existence and rapidly deployed. Limited testing is being conducted before technologies are launched at scale. The testing is lab-based or simulated rather than 'in the wild' and concerned with whether the technology functions, rather than whether it is an effective solution or its other effects. Surveillance technologies then are being adopted without it being clear whether they are a suitable and viable means to delay and contain the spread of the virus. Indeed, key questions overlooked in the hype to promote technology-led solutions are whether they are fit-for-purpose and will they produce the intended outcomes? Here, I consider these questions with respect to smartphone-based contact tracing and quarantine enforcement (digital fences)/travel permission (digital leashes).

Technical feasibility and validity

The rationale for using automated contact tracing via cell/smartphone technology is that it will be possible to significantly expand the volume and reach of traditional contact tracing, which is time consuming, labour-intensive and costly, relies on memory, and cannot identify proximate strangers (Stokel-Walker, 2020). By calculating the close proximity of phones, the intersections of millions of people can be automatically traced, including contacts with people who subsequently test positive. Since cell-site location information

Table 1. Issues arising from the use of surveillance technologies for tackling the spread of COVID-19.

Technical/practical	Civil liberties and governmentality	Surveillance capitalism
• Technological solutionism • Robust, domain-informed design • Pilot testing and quality assurance • Fit-for-purpose • Rule-set and parameters • Potentially fragmented data sources • Data coverage and resolution • Representativeness and digital divides • Data quality, reliability and false negatives/positives • Duping and spoofing • Dependent on effective virus testing and certification • Contact tracing dependent on 60% participation; • Quarantining/travel permissions can require additional infrastructure • Firm legal basis • Proof more effective than traditional contact tracing	• Individual rights vs public good • Privacy, data leakage, re-identification • Data minimization and consent • Governmentality • Social/spatial sorting, redlining • Population profiling • Control creep • Normalization • Authoritarianism • Due process, oversight, redress • State record on dataveillance • Public trust and chilling effects	• State-sanction surveillance capitalism • New market opportunities • Gateway to public health and other state data • Deepening data shadows • Enrolment of new smartphone owners • Covidwashing of activities • Increasing shareholder value and profit

(CSLI) based on connections to nearby towers is too coarse and wifi connections are too partial in coverage outside of densely urbanized places, the focus has been on GPS to monitor shared location and Bluetooth to record close contacts (Stanley & Granick, 2020). However, GPS nor Bluetooth have strong spatial precision.

The recommendation of most governments is to avoid close and prolonged contact with others, maintaining a social distance of 2 metres or more. Accurately and reliably determining less than 2 metres proximity and length of infringement is not possible. GPS can have an accuracy up to 1 metre, but more typically it is 5–20 metres, and the technology does not work indoors, works poorly in the shadow of large buildings and during thunderstorms and snowstorms, and establishing location can take several minutes when the device is first turned on or brought outdoors (Schwartz & Crocker, 2020; Stanley & Granick, 2020). Bluetooth does not calculate location, but enables communication with other devices up to a range of 30 metres. The nearness of other phones can be estimated using the Received Signal Strength Indicator (RSSI), but that lacks accuracy and varies with conditions (such as being in a bag or pocket) (Leith & Farrell, 2020). Moreover, not all phones have Bluetooth turned on by default and its use is a significant drain on battery life (Stanley & Granick, 2020). GPS nor Bluetooth can determine if there is a wall or window between people and they are sharing the same airspace. In order to exclude fleeting and seemingly meaningless encounters, systems use a time element. In the proposed UK app, a person will only be recorded as a close contact if their device has been within 2 metres proximity to another for 15 minutes or more (Kelion, 2020). However, this has the effect of excluding brief, but potentially significant, encounters such as a person passing in a supermarket aisle sneezing, or sitting near someone coughing on a bus for 10 minutes.

The rationale for using digital fences and leashes is that they provide a robust and rapidly scalable means for individualized movement control. There are two predominant means to implement digital fences to prevent movement. The first is to monitor whether a mobile phone or electronic tag has left a domicile through GPS tracking. The second is to use automated messaging requiring the respondent to reply with a geo-located message within a short timeframe. Digital leashes that provide limited permission to move are implemented by issuing QR codes that are scanned and verified at access points. It thus requires the rolling out of a dense network of checkpoint infrastructure across buildings, public space and public transit. Such infrastructure is presently absent in most jurisdictions. Another method is to scan people's body temperatures to verify that they do not have a fever and can enter a space. However, thermal cameras only have moderate accuracy, with FLIR, an industry leader, reporting a potential margin of error of 3.6 degrees Fahrenheit above or below a person's true temperature (Gershom, 2020).

There are other technical issues that raise doubts about the efficacy of using technology-mediated contact tracing and digital fences and leashes. There are, for example, general concerns around data quality. Big data – voluminous streams of real-time data – are often noisy and messy, with gaps, errors, biases, and inconsistencies that prompt questions of veracity (accuracy and precision) and reliability (consistency over time) (Kitchin, 2014). When decisions are made on inaccurate and unreliable data that will limit personal freedoms, processes must be put in place to ensure that quality is as high as possible (McDonald, 2020). There is little evidence that such processes are actively being implemented. Moreover, elements of some system designs create the potential to downgrade quality.

For example, the subjective nature of self-diagnosis will introduce false positives based on suspected but not actual cases. Moreover, it is possible to dupe and spoof systems wherein pertinent data is omitted or false data added. People could choose to turn off the location function on their phone, or not turn on Bluetooth, or leave their phone at home, or use a secondary device, or borrow someone else's (Stanley & Granick, 2020). Alternatively, they might decide not to share information if they are experiencing symptoms, or decide to avoid taking a test. As Teresa Scassa notes:

> As we try to return to normal, there's going to be such an incentive for people to game the app. You have to get back to work and support your family. Are you going to be telling an app that you have a cough? (Patriquin, 2020)

In addition, because Bluetooth signals are vulnerable to spoofing, it is possible for someone to grab the ID code and broadcast it in a different location (Angwin, 2020).

Data coverage and representativeness raise further issues. Unless there is a central, single app through which all contact tracing occurs, then location data – especially when based on GPS and app-harvested data – are fragmented across telecommunications providers or location tracking companies, and also are stored in different formats making joining them together tricky. This is particularly an issue in the US and other countries where private companies have offered to perform contact tracing or flow modelling (Stanley, 2020). In the case of Apple and Google's initiative, the data only relate to smartphones using Android and iOS and exclude cell phones – a problem given 19% of Americans do not own smartphones and among the high-risk coronavirus group, those aged 65 +, the rate increases to 47% (Pew Research, 2019). There are also differentials across class and race. 29% of Americans who earn less than $30,000 per annum do not own a smartphone (Pew Research, 2019), which makes contract tracing within this group less effective (Schwartz & Crocker, 2020) and any introduction of a QR-based system for approved movement would mean almost a third of low-income workers being digitally fenced-in unless they invest in a smartphone. And some religious groups opt-out of smartphone use, for example, some Jewish denominations and the Amish (Ems, 2015). In addition, to work effectively, the technologies require all smartphone users to have them charged, turned on, and with them at all times.

Beyond questions about data quality and coverage, there are questions about the algorithms and rule-sets used to interpret and make decisions based on these data. As Julia Angwin (2020) notes, systems need to implement a robust and reliable means of identifying possible transmission and cannot be so trigger happy that they overload users with false alerts. At the same time, they cannot be too cautious that a genuine risk is ignored. Besides negative outcomes for close contacts, false positives would also pose a risk of overloading the testing system, especially if that was the only means of exiting any measures imposed via contact tracing. They would also weaken trust in the system, potentially leading to users to ignore instructions (Angwin, 2020). In Israel, people who were mandatorily isolated – but not tested – based on contract tracing have protested against the use of the system, finding it difficult to get mistakes corrected (Linder, 2020). Thus, as the American Civil Liberties Union (ACLU) states:

> Using the wrong technology to draw conclusions about who may have become infected might lead to expensive mistakes such as two week isolation from work, friends, and

> family for someone — perhaps even a health care worker or first responder — who was actually not exposed. (Stanley & Granick, 2020)

Critical conditions

It is clear that the tech-based solutions being pursued and deployed are far from ideal and have a number of issues that suggest they may not be fit-for-purpose. But even if they are suitable, it is important to note that they will *only be effective* in practice if:

(1) there is a programme of mass testing, with certification, to confirm that a person has the virus and if tracing or digital fencing/leashing is required (Angwin, 2020);
(2) the number of cases is low, R<1, and selectively isolating cases (as opposed to mass isolation) will be effective at limiting rapid growth;
(3) 60% of the population participate in contact tracing (Stokel-Walker, 2020; Kelion, 2020); there is full compliance and adequate policing of quarantining/travel permissions.
(4) there is a firm legislative basis for deployment of technology-led solutions (Ada Lovelace Institute, 2020).

Without an extensive regime of testing with certification, known documented cases to trace from will be absent. In addition, an unknown number of undocumented carriers will continue to circulate, undermining the effects of tracing/quarantining. In situations where there have been a large numbers of cases, app-based contact tracing will only be effective once the rate of transmission (R) is below one and near zero to potentially limit any additional waves of infections. The UK proposed solution to a lack of mass testing is to allow people to self-diagnose via a questionnaire and not have to speak to a health advisor or obtain a test result (Kelion, 2020). This is likely to lead to an enormous number of false negatives/positives.

Developers suggest that for phone-based contact tracing systems to be effective they would require c.60% of the population to participate (equivalent to c.80% of smartphone owners in the UK) (Kelion, 2020; Stokel-Walker, 2020). In Singapore, where using the TraceTogether app was voluntary, only 17% of the population had installed it after a month (Vaughan, 2020), suggesting that gaining a 60% adoption rate elsewhere will be a challenge. While emergency powers in a state of exception have been invoked to put in place traditional containment measures, making the app mandatory (for example required to be exempt from lockdown measures) will likely be subject to legal challenge (Stanley, 2020; Stokel-Walker, 2020) and met with resistance and subversion in democratic countries. Similarly, quarantine enforcement and travel permission technology will likely be resisted by populations in non-authoritarian states and it would require necessary infrastructure to be put in place, though companies might embed it into their governmental practices for their workers and visitors, thus starting to normalize its use.

Civil liberties, governmentality, and surveillance capitalism

Beyond technical and practical feasibility issues, the consequences of deploying these technologies appear to have been little considered prior to commissioning, or were deemed to have acceptable downsides to be suffered for the greater good.

The issue that most critical commentary has focused upon is privacy, since the technologies demand fine-grained knowledge about movement, social networks and health status (Angwin, 2020; Schwartz & Crocker, 2020; Stanley & Granick, 2020). For initiatives where contact tracing leverages off of existing location tracking by private enterprises – such as location marketing firms and adtech – and does not involve consent, there is clearly a breach of the data minimization principle: that only data relevant and necessary to perform a task are generated and these are only used for the purpose for which they were produced (OECD, 1980; Information Commission's Office, n.d.). In opt-in and consent based initiatives, developers have sought to reassure users that any location tracking and/or contact tracing would not collect data on or share people's identities, using anonymous IDs. In centralized systems the data would be stored on government servers, which would be protected by cybersecurity measures. In decentralized systems, nearly all the data would be stored on users' phones, with privacy advocates favouring this approach. Both approaches provide the potential for data to be leaked or filter into other apps on a user's phone, or for IDs to be captured by other apps on other nearby users' phones, or via communications with central servers (Angwin, 2020). These data could then be shared with third parties (Patriquin, 2020). Moreover, by opening up location data, either via GPS or Bluetooth, a device is being made trackable by a range of adtech embedded in other apps, enrolling it into the ecosystem of location-based data brokers (Angwin, 2020). For companies, such as Palantir which is modelling using contact tracing data for governments, it is not clear whether the data are being added to their already sizable databanks and to individual profiles, and repurposed in other work.

In addition, there have been concerns that data could be re-identified, undoing the process of anonymization.[8] Indeed, it is well established in the big data literature that unless the data are fully de-identified it is possible to reverse engineer anonymisation strategies by combing and combining datasets (de Montjoye et al., 2013; Narayanan & Shmatikov, 2010). In South Korea, for example, it proved straightforward to re-identify early patients (Singer & Sang-Hun, 2020). The same was true for Singapore, where the personal details of those testing positive, including gender, age, workplace and relationship to other cases, were published on the Health Ministry's website (Singer & Sang-Hun, 2020). Similarly, Hong Kong provides an interactive map that displays every case by building, listing the age, resident status, dates of virus onset and confirmed by testing, whether imported or community transmission, and hospital if admitted.[9] De-identification requires both direct identifiers and quasi-identifiers (those highly correlated with unique identifiers) to be carefully removed (Cavoukian & Castro, 2014). The extent to which this is happening, or will happen, is not clear.

The implications for privacy are worrying enough for many; however, the consequences extend to governmentality and civil liberties more generally (even if privacy is protected). Contact tracing and movement monitoring are designed to rescript how we live our lives, reshaping social contact and movement (Aouragh et al., 2020). They socially and spatially sort, redlining who can and cannot mix, move and access spaces and services. As Aouragh et al. (2020) note, contact tracing apps:

> will be laying out normative conditions for reality, and will contribute to the decisions of who gets to have freedom of choice and freedom to decide … or not … and will co-define who gets to live and have a life, and the possibilities for perceiving the world itself.

The various surveillance technologies being deployed are designed to implement disciplining (nudging people to comply with social distancing for fear of the consequence of close contact) and control (actively prescribing spatial behaviour, where there is little choice but to comply) forms of governmentality. As such, along with traditional containment measures, and the power of the communal gaze and shaming, the technologies seek to produce docile, compliant bodies (Foucault, 1991). More than that though, their technocratic, algorithmic, automated nature can shift the governmental logic from surveillance and discipline to capture and control (Deleuze, 1992), wherein people become subject to constant modulation through data-driven systems in which their behaviour is directed explicitly or implicitly steered rather than (self)disciplined (Kitchin, 2018). This biopolitical power is deepened through the present state of exception (Agamben, 2005), where usual rights are suspended and measures are imposed without the customary checks and balances as legitimate actions of good government for collective benefit (Avila, 2020).

This emerging pandemic biopolitics is centrally concerned with the close management and control of bodies and their circulation and contact; it is thoroughly spatial in its articulation, regulating public and private spaces, spatial access and behaviour, and producing particular spatialities. Importantly, the constructed dispositive (institutions, bureaucracy, infrastructure, regulation, laws, and discursive regime; Foucault, 1977) is extending beyond public space to become a feature of workplaces (e.g. temperature testing, certified status, or the use of contract tracing app to access work spaces; and monitoring a range of performance metrics including keystrokes, emails sent, and status updates of those home working) (Mosendz & Melin, 2020). Moreover, as the ACLU, EFF and others have pointed out, the risks of exposure and application of governmental practices are unevenly applied across populations, particularly given the demographics of 'essential workers' in retail, service, distribution industries and public health and the wider public sector. As with algorithmic governance in general, this unevenness and inequity is reproducing data justice issues (Dencik et al., 2016; Taylor, 2017) across class, race, ethnicity and gender (Benjamin, 2019; Eubanks, 2018; Noble, 2018) with potentially lethal consequences.

To enable this new biopolitical architecture, existing technologies such as smartphone infrastructure are being subject to control creep (Innes, 2001); that is, their original purpose is being extended to perform surveillance and governance work. This creep while optional in some cases (e.g. the use of contract tracing apps) might shift to become mandatory (though not necessarily compulsory). For example, some companies might make using an app necessary to access workspaces, or states might make its use a condition of lifting restrictions (Weaver, 2020). This is already occurring in India where the contact tracing app, Aarogya Setu, will be mandatory for those living in containment zones and for all public and private sector employees (Sircar & Sachdev, 2020). Failure to install the app will lead to a fine or prison term. Over the past two decades, particularly post 9/11, control creep has been occurring across networked systems, with technologies designed to deliver specific services being enrolled into policing and security apparatus (Kitchin and Dodge, 2011). While in the present crisis control creep is occurring and being sought for the purposes of public health, the danger is that its use will normalize government tracking and digital fencing/leashing, with the architectures developed subsequently used with respect to on-going health monitoring and pivoting to other issues such as policing, emergency management response, and national security (Sadowski,

2020). For example, the fear is that the Indian app will be repurposed for political ends to monitor and discriminate against certain populations. Certainly, the control creep that happened post 9/11 was not subsequently rolled back (McDonald, 2020; Sadowski, 2020).

With good reason then, there are fears that the systems deployed to tackle the pandemic will not be turned off after the crisis, instead becoming part of the new normal in monitoring and governing societies (Sadowski, 2020; Stanley & Granick, 2020). As French and Monahan (2020) note in their overview of how surveillance technologies have historically been enrolled into disease control, technology solutions tend to persist. In other words, any technologies implemented now are likely to act as gateways to a new type of management that routinize a new form of social and spatial sorting. This has the potential to permanently shift the nature of governmentality and to also act as a pathway towards authoritarian forms of governance where technology is used to actively impose the will of the state onto citizens. The fine-grained mass tracking of movement, proximity to others, and knowledge of some form of status (beyond health, for example) will enable tighter forms of control and is likely to have a chilling effect on protest and democracy. Such a pathway is legitimized because, as Jathan Sadowski notes, 'authoritarianism – for the "right" reasons – starts looking tolerable, even good, because it looks like the only option' (Sadowski, 2020). As Snowden, Wikileaks, and numerous other investigations have shown, states have a poor record at practicing dataveillance (Lyon, 2015), which lend a legitimacy to such concerns.

China and Russia provide some clues as to what this could mean, and while some advocates might point to China as an example where technology solutions to the coronavirus have seemingly worked, it also raises alarm bells. As an authoritarian state, China was well able to perform a lockdown through social and state policing without technology support. However, it could quickly mobilise technology solutions because it is already well down the road of implementing Big Brother style surveillance apparatus through social credit scoring and pervasive smart city tech, including millions of facial recognition and automatic number plate recognition cameras (Keegan, 2019; Lee, 2019; Liang et al., 2018). Smartphones have become an essential technology for daily life, not least because in the move to a cashless society they have become virtual wallets, and a means to trace all digital transactions (Mozur, 2017). From December 2019, all mobile phone users registering new SIM cards in China have had to provide a facial recognition scan, creating a direct biometric link between person and phone (Kuo, 2019). The pandemic crisis was an opportunity for the state to further roll-out and normalize surveillance technologies and there is little sense that the tracking implemented there will be rolled-back post-crisis. In other words, the tech may have had limited effects beyond social and governance measures being implemented that confined people to homes, but had significant downstream effects. Spatial sorting through app-approved entrance to public and private spaces may well become the new normal. The same is feared in Russia, where critics have dubbed the Moscow lockdown enforcement app the 'Cyber Gulag' (Ilyushina, 2020).

In addition, there are concerns around the legality of systems, the extent to which they will pronounce recommendations or compulsory orders, and be accompanied by practices of due process, oversight, and the right to redress and to opt-out (McDonald, 2020). If one does opt-in to using a contact tracing app, will it be compulsory to share a positive test result through the app? Or if the app informs a person that they have been in close proximity to someone who has tested positive, will they have to undertake the measures it

diagnoses? Will there be penalties for flagrantly ignoring instructions? Would it make a difference if the instruction is based on testing or self-diagnosis? It would be particularly difficult to try and justify following instructed measures without a robust and extensive testing regime and certification in operation. In cases where the instructions are to be compulsory will there be a means to appeal them? Can people opt back out of the scheme once enrolled? Would there be any penalties for doing so? Will there be a formal mechanism for overseeing the implementation and operation of new tech developments to ensure that they adhere to existing regulations and legislation and do not abuse the power vested in the initiative? Are there associated penalties for any irregularities or abuses? There has been precious little evidence that these questions have been thought through and that due process and oversight are being put in place (McDonald, 2020).

In addition, by pursuing surveillance based solutions in collaboration with industry, either through procurement or partnership, the methods and logics of surveillance capitalism (Zuboff, 2019) are legitimated and reproduced. As has been well documented in the surveillance studies literature, over the past two decades there has been a significant step change in individual level, fine-grained data harvesting and profiling, and enormous expansion in the number of data brokers and their profits (Kitchin, 2014). In particular, the advent of the smartphone in the mid-2000s has led to a bonanza of indexical, real-time location-based data harvested through apps that record and transmit location, with 58 companies specializing in location tracking operating in the US alone in 2014 (Angwin, 2014), which has since grown. In addition, telecommunication companies, social media companies such as Facebook (includes Whatsapp and Instagram), as well as Apple, Google and Microsoft that provide smartphone operating systems are generating and storing real time location and movement data. While many have known that these companies are producing such data, the COVID-19 pandemic has laid it bare through the offers of these companies to share data and analytic tools to aid contact tracing, monitor the effects of social distancing, and perform movement monitoring.

While undoubtedly many of these companies have been motivated by a desire to help during a pandemic crisis, it is also clear that such a move has other effects and motivations. First, it helps legitimate surveillance capitalism and the invasive harvesting and exploitation of people's data for profit. In effect, these activities, especially when provided pro bono, enable the 'covidwashing'[10] of surveillance capitalism through the laundering of reputations (McDonald, 2020; Stanley, 2020). While unintentional, the adoption of company solutions by states are also helping to boost shareholder value and investor profits. Second, it provides an opportunity for these companies to promote and market their activities and services and potentially attract future business. Third, it opens up potential new products and markets. In a call to investors, Phunware – a smartphone tracking company that is part of Trump's 2020 re-election campaign – made clear the motivation for engaging with the pandemic, pitching several potential new products and markets, including social distance policy enforcement (Biddle & Fang, 2020). No doubt some companies hope that contributing to the effort to tackle COVID-19 will act as a gateway to public health and other government contracts (Sadowski, 2020), as well as to the further privatization of public health data. Fourth, it is further increasing and deepening data shadows, either through gaining access to new data or encouraging the enrolment of new smartphone owners. A clear concern, then, is that the COVID-19 pandemic will

cement and normalize the practices of surveillance capitalism, which has done much to undermine civil liberties related to privacy, social and spatial sorting, and profiling.

Public health *or* civil liberties, or public health *and* civil liberties?

The discussion so far has highlighted that: the surveillance technologies being used have been rushed to deployment and their fit-for-purpose has not been established; there are significant implications for civil liberties, governmentality and citizenship from using these technologies; and citizens are being asked to trade civil liberties for public health via the use of unproven or error-prone surveillance technologies. While some might claim that the urgency of the situation and the severity of the disease demands that public health trumps civil liberties and the price is increased surveillance, altered governmentality, and a strengthening of surveillance capitalism (Tony Blair Institute for Global Change, 2020), this is too simplistic for three reasons.

First, the trade might be a false one if the surveillance technologies cannot deliver the anticipated public health benefits, meaning there are no commensurate benefits arising from their use (Stanley & Granick, 2020). This is the conclusion of the American Civil Liberties Union (ACLU) (Guarglia & Schwartz, 2020) and The Ada Lovelace Institute (2020), the latter of which concludes with respect to contact tracing that '[t]here is currently insufficient evidence to support [its] use … [t]he technical limitations, barriers to effective deployment and social impacts demand more consideration'.

Second, the mind-set of trading of civil liberties for public health is rooted in technological solutionism, wherein technology is seen as the only viable solution to resolve an issue regardless of ancillary costs, and policy is led by technology rather than vice-versa (Morozov, 2013). Many states have become primed for pursuing technological solutionism through successive waves of lobbying by tech companies, their own turn towards technocratic practices, and their desire to stimulate innovation in high-tech sectors of the economy. They have therefore been amenable to the solutionist proposition that mass surveillance or tech-mediated control should be a primary means for beating the disease (Aouragh et al., 2020). Such a systems-thinking, deterministic approach, rather than a socio-technical view, forecloses any wider consideration of whether it is the most appropriate or effective solution and what its unanticipated effects or wider cost/benefits might be. Instead, when shortcomings are highlighted, the response is framed as: 'using the tech, even if flawed or unsuitable, is better than not using it', regardless of any externalities, or whether the critical conditions exist for it to be successfully deployed. The result is a rush to implement first and to continue to push ahead with deployments even when the shortcomings are evident.

Third, it is possible to push for deployments that respect issues like privacy and control creep, ensuring civil liberties *and* public health (Goldenfein et al., 2020). In fact, not ensuring civil liberties is likely to undermine public health efforts by eroding trust and encouraging dissent (Ada Lovelace Institute, 2020). In Korea and Singapore where early patients were re-identified they were publicly hounded and shamed, having a chilling effect on testing (Singer & Sang-Hun, 2020). Rates of adoption of contact tracing apps are low, in part because people do not trust the government's past record concerning personal data (Patton, 2020). If people feel their rights are being infringed or they are being managed or targeted in ways they do not like or

trust then they will opt-out of the technology, or find ways to circumvent and subvert it, or avoid testing or seeking health care (Schwartz & Crocker, 2020). This will especially be the case for those who may not have the means and social supports from the state to stay socially isolated. As Anna Johnston (2020) notes, appealing to nationalistic pride, or threatening to block the lifting of restrictions or to make usage mandatory, or blithely arguing that the state or Google/Facebook and others already know everything about us, is likely to be counterproductive. Instead, public education and voluntary measures and compliance are more effective than law enforcement approaches in tackling public health issues (Stanley & Granick, 2020), and any heavy-handed measures are likely to 'sour the relationship between citizens and their government when trust is of paramount importance' (Schwartz & Crocker, 2020). There is a danger then that the technologies will have the opposite effect to that desired.

To try and ensure that civil liberties are not unnecessarily traded for public health, organizations and academics in a number of jurisdictions have been running active campaigns. Their central message is that if surveillance technologies are to be deployed then they should be appropriate, proportionate, comply with existing legislation, and protect civil liberties. For example, the Electronic Frontier Foundation, American Civil Liberties Union, the Ada Lovelace Institute,[11] and the European Data Protection Board[12] demand that:

- data collection and use must be based on science and need;
- the tech must transparent in aims, intent, and workings;
- the tech and wider initiative must have an expiration date;
- a privacy-by-design approach with anonymization, strong encryption and access controls should be utilized;
- tools should ideally be opt-in and consent sought, rather than opt-out, with very clear explanations of the benefits of opting-in, operation and lifespan;
- the specification and user requirements, a data protection/privacy impact assessment, and the source code must be published;
- data cannot be shared beyond the initiative or repurposed or monetized;
- no effort should be made to re-identify anonymous data;
- the tech and wider initiative must have proper oversight of use, be accountable for actions, have a firm legislative basis, and possess due process to challenge mis-use.

What these demands mean is that the tools must only be used when deemed necessary by public health experts for the purpose of containing and delaying the spread of the virus and their use discontinued once the crisis is over. Citizens should know precisely what the technologies seek to achieve and what will happen with their data. There should also be safeguards to stop control creep and the technology being repurposed for general or national security, predictive policing or other governance or commercial purposes. In addition, their development should be guided by detailed user requirements set by public health and privacy experts and not left to amateurs or private companies to lead design and production. In this regard, technology developed through hackathons where participants lack domain knowledge are unlikely to be of use even if they can subsequently be re-configured to meet legal, social and political expectations. As a result of this lobbying, a number of countries have altered their design specifications and architecture of their

contact tracing apps during their development, swapping from a centralized to decentralized approach to deal with concerns related to privacy and data protection (Busvine & Rinke, 2020; O'Brien, 2020). Equally, there has been push back against the use of other surveillance technologies such as drones, facial recognition cameras, and biometric monitoring given their invasive nature and little evidence of effective performance beyond traditional measures such as social distancing.

Conclusion

My aim in this paper has been to provide a relatively broad overview of the technical, practical, and ethical issues of developing and deploying surveillance technologies to delay and containment measures for tackling COVID-19. My primary focus has been on contact tracing, quarantine enforcement and travel permission using smartphone technologies and there is a need to extend a more thorough analysis to social distancing/movement monitoring and symptom tracking, and the use of facial recognition and thermal cameras, biometric wearables, drones, and predictive analytics. The analysis highlights that in the rush to act quickly there has not been sufficient thought and assessment given to the technical feasibility of proffered solutions, whether they will work in practice, and the extent to which they will provide more effective outcomes than traditional interventions. Nor has there been sufficient consideration of their consequences for civil liberties, biopolitics or surveillance capitalism and whether the supposed benefits outweigh any commensurate negative effects, or whether the public health ambitions can be realized while protecting civil liberties.

The initial assessments of the technology solutions being proposed and deployed suggests that their utility has been oversold. Smartphone based contact tracing will be ineffectual without mass testing (not self-diagnosis), it ideally needed to be introduced when the number of infections were very low, and it requires a 60% opt-in rate which is unlikely to be achieved. Quarantine enforcement and travel permission technology will be unpalatable to many citizens and used reluctantly, and will be resented, resisted and subverted. And while governments and companies have sought to reassure about the effects of these solutionist technologies on civil liberties, it is clear that they do have profound implications for privacy, governmentality, control creep, and citizenship, and they do reinforce the logic of surveillance capitalism.

As the response to the crisis unfolds there is a need for geographers and others to document the ways in which a new surveillance and biopolitical regime is being produced through the alliance of government control and surveillance capitalism and their use of a range of technologies. This work needs to unpick the epistemic communities and advocacy coalitions being formed (Kitchin et al., 2017) and the biopolitics and dispositive they construct and mobilize to promote technology-led solutions (Avila, 2020), and chart how the technologies are being deployed in practice, their effects on public health and civil liberties, governmentality and citizenship, and the extent to which they creep, become mandatory, and defy sunset clauses that end their use. Importantly, this work needs to examine how these technology-led solutions are unfolding across jurisdictions given the different political economies and regimes. Indeed, the kinds of technology-led solutions being deployed in the Global North might be quite different to the Global South, where even traditional public health measures might be difficult to practice

given the challenges of performing and economic costs (Taylor, 2020). Moreover, there is a need to examine the application and effects of these emerging surveillance regimes on different communities, their effects across class, race, ethnicity, gender and other social groups, and to chart how people are resisting, subverting and seeking to enact forms of data justice. In addition, there is a need to extend the lens of analysis beyond public space to focus on the use of surveillance technologies and emerging governmentalities in the workplace.

As we conduct this research we need to be persistent in stressing that civil liberties and public health do not need to be traded against each other, but must work in harmony if we are to create a just and fair society in the pandemic's wake.

Notes

1. For example, in Ireland Science Foundation Ireland, Enterprise Ireland and the IDA Ireland launched a joint rapid-response call to fund research and innovation activities to develop solutions that can have demonstrable impact on the tackling the virus. https://www.irishtimes.com/news/science/urgent-call-out-for-irish-scientists-to-help-global-coronavirus-response-1.4217710
2. For example, the EU vs Virus hackathon, https://euvsvirus.org/; The Global Hack, https://theglobalhack.com/; an example of more bottom event is the Codevid Hackathon, https://codevid19.com/
3. Global Positioning System
4. In late April the Israeli Supreme Court banned its intelligence agency from tracing the phone location of those infected with Covid-19 until new legislation is passed. https://www.bbc.com/news/technology-52439145
5. Also see: https://en.wikipedia.org/wiki/COVID-19_apps
6. https://www.google.com/covid19/mobility/
7. https://twitter.com/WolfieChristl/status/1246079249544630279
8. See https://twitter.com/ashk4n/status/1250071326372638736 for an example of how this might be done.
9. https://chp-dashboard.geodata.gov.hk/covid-19/en.html
10. https://twitter.com/WolfieChristl/status/1242956802930683913
11. Ada Lovelace Institute (2020); Guarglia and Schwartz (2020); Stanley (2020)
12. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

Acknowledgements

I am grateful for the feedback of Alistair Fraser, Tracey Lauriault and Sophia Maalsen, along with two anonymous referees, on earlier drafts of this paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Science Foundation Ireland [Grant number 15/IA/3090].

Notes on contributor

Rob Kitchin is a professor of human geography at Maynooth University, Ireland. His research focuses on the relationship between digital technologies, society and space. He is (co)author or (co)editor of 30 academic books, numerous articles and book chapters, and is an editor of the journal Dialogues in Human Geography. https://www.maynoothuniversity.ie/people/rob-kitchin.

ORCID

Rob Kitchin http://orcid.org/0000-0003-4458-7299

References

Ada Lovelace Institute. (2020). *Exit Through The App Store*. April 20, https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-1.pdf

Agamben, G. (2005). *States of exception*. University of Chicago Press.

Angwin, J. (2014). *Dragnet Nation*. St Martin's Press.

Angwin, J. (2020). Will Google's and Apple's COVID Tracking Plan Protect Privacy? *The Markup*, 14 April. https://themarkup.org/ask-the-markup/2020/04/14/will-googles-and-apples-covid-tracking-plan-protect-privacy

Aouragh, M., Pritchard, H., & Snelting, F. (2020). The long tail of contact tracing. D3PT (Decentralized Privacy-Preserving Proximity Tracing). *GitHub*, April 10. https://github.com/DP-3T/documents/issues/118

Avila, K. (2020). Coronavirus as a dispositive. *Open Democracy*, May 4, https://www.opendemocracy.net/en/democraciaabierta/coronavirus-dispositive/

Benjamin, R. (2019). *Race after technology*. Polity Books.

Biddle, S., & Fang, L. (2020). Location-Tracking Firm Helping Trump Get Reelected Now Wants to Cash In on Coronavirus. *The Intercept*, April 9. https://theintercept.com/2020/04/09/coronavirus-trump-smartphone-tracking/

Brandom, R., & Robertson, A. (2020). Apple and Google are building a coronavirus tracking system into iOS and Android. *The Verge*, April 10, https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app

Busvine, D., & Rinke, A. (2020). Germany flips to Apple-Google approach on smartphone contact tracing. *Reuters*, April 26, https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J

Cahane, A. (2020). The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers. *Lawfare*, March 21. https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers

Cavoukian, A., & Castro, D. (2014). *Big data and innovation, Setting the record Straight: De-identification does work*. Information and Privacy Commissioner Ontario. www2.itif.org/2014-big-data-deidentification.pdf

Deleuze, G. (1992). Postscript on the societies of control. *October*, *59*, 3–7.

de Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Nature, Scientific Reports*, *3*, 1–5. Article 1376. https://doi.org/10.1038/srep01376

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society*, *3*(2), 1–12. https://doi.org/10.1177/2053951716679678

The Economist. (2020). Countries are using apps and data networks to keep tabs on the pandemic. *The Economist*, March 26. https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic

Ems, L. (2015). Exploring ethnographic techniques for ICT non-use research: An Amish case study. *First Monday*, *20*(11). https://doi.org/10.5210/fm.v20i11.6312. https://journals.uic.edu/ojs/index.php/fm/article/view/6312/5139

Eubanks, V. (2018). *Automating Inequality: How high-tech tools Profile, police, and Punish the poor*. St Martin's Press.

Foucault, M. (1977). The confession of the flesh. In C. Gordon (Ed.), *(1980) power/knowledge* (pp. 194–228). Pantheon Books.

Foucault, M. (1991). Governmentality. In G. Burchell, C. Gordon, & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87–104). University of Chicago Press.

Fowler, G. A. (2020). Smartphone data reveal which Americans are social distancing (and not). *Washington Post*, March 24. https://www.washingtonpost.com/technology/2020/03/24/social-distancing-maps-cellphone-location/

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies Address COVID-19? *Surveillance Studies*, *18*(1), 1–11. https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/13985

Gershom, D. (2020). Infrared Cameras Could Be the New CCTV. *OneZero*, April 24. https://onezero.medium.com/infrared-cameras-could-be-the-new-cctv-b4c79ede310e

Goh, B. (2020). China rolls out fresh data collection campaign to combat coronavirus. *Reuters*, February 26. https://www.reuters.com/article/us-china-health-data-collection/china-rolls-out-fresh-data-collection-campaign-to-combat-coronavirus-idUSKCN20K0LW

Goldenfein, J., Green, B., & Viljoen, S. (2020). Privacy Versus Health Is a False Trade-Off. *Jacobin*, April 17. https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology

Guarglia, M., & Schwartz, A. (2020). *Protecting civil liberties during a public health crisis*. Electronic Frontier Foundation, March 10. https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

Hatmaker, T. (2020). Palantir provides COVID-19 tracking software to CDC and NHS, pitches European health agencies. *Tech Crunch*, April 1. https://techcrunch.com/2020/04/01/palantir-coronavirus-cdc-nhs-gotham-foundry/

Hoonhout, T. (2020). Kansas Says It's Using Residents' Cell-Phone Location Data to Fight Pandemic. *National Review*, April 1. https://www.nationalreview.com/news/coronavirus-kansas-using-resident-cell-phone-location-data-fight-pandemic/

Ilyushina, M. (2020). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a 'cyber Gulag'. *CNN*, April 14. https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html

Information Commission's Office. (n.d.). *Principle (c): Data minimisation*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/

Innes, M. (2001). Control creep. *Sociological Research Online*, *6*(3). http://www.socresonline.org.uk/6/3/innes.html

Johnston, A. (2020). Should I download the COVID-Safe app? The privacy pros and cons. *Salinger Privacy*, April 29. https://www.salingerprivacy.com.au/2020/04/29/covidsafe-app-blog/

Jones, S. (2020). Liechtenstein rolls out radical Covid-19 bracelet programme. *Financial Times*, April 16. https://www.ft.com/content/06b7e6f3-a725-4eda-9153-e0af48040e30

Keegan, M. (2019). Big Brother is watching: Chinese city with 2.6 m cameras is the world's most heavily surveilled. *The Guardian*, December 2. https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

Kelion, L. (2020). Coronavirus: NHS contact tracing app to target 80% of smartphone users. *BBC News,* April 16. https://www.bbc.com/news/technology-52294896

Kitchin, R. (2014). *The data Revolution: Big data, Open data, data Infrastructures and their consequences*. Sage.

Kitchin, R. (2018). Governance. In J. Ash, R. Kitchin, & A. Leszczynski (Eds.), *Digital Geographies* (pp. 238–249). Sage.

Kitchin, R., Coletta, C., Evans, L., Heaphy, L., & Mac Donncha, D. (2017). Smart cities, urban technocrats, epistemic communities, advocacy coalitions and the 'last mile' problem. *IT – Information Technology*, *59*(6), 275–284. https://doi.org/10.1515/itit-2017-0004

Kitchin, R., & Dodge, M. (2011). *Code/space: Software and Everyday life*. MIT Press.

Kuo, L. (2019). China brings in mandatory facial recognition for mobile phone users. *The Guardian*, December 2. https://www.theguardian.com/world/2019/dec/02/china-brings-in-mandatory-facial-recognition-for-mobile-phone-users

Lee, C. S. (2019). Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review*, *43*(6), 952–970. https://doi.org/10.1108/OIR-08-2018-0231

Leith, D. J., & Farrell, S. (2020). Coronavirus contact tracing: Evaluating the Potential of using Bluetooth received signal strength for proximity detection. April 6. https://www.scss.tcd.ie/Doug.Leith/pubs/bluetooth_rssi_study.pdf

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy and Internet*, *10*(4), 415–453. https://doi.org/10.1002/poi3.183

Linder, R. (2020). Quarantined After Waving at Coronavirus Patient: How Accurate Is Israel's 'Terrorist-tracking' Tech? *Haaretz*, March 22. https://www.haaretz.com/israel-news/.premium-isolated-after-waving-at-corona-patient-is-israeli-phone-tracking-tech-accurate-1.8698946

Linklaters. (2020). 28 countries race to launch official Covid-19 tracking apps to reduce the spread of the virus. April 16. https://www.linklaters.com/en/about-us/news-and-deals/deals/2020/april/28-countries-race-to-launch-official-covid-19-tracking-apps-to-reduce-the-spread-of-the-virus

Lyon, D. (2015). *Surveillance after Snowden*. Polity Press.

Martin, A. (2020) Coronavirus: NSO Group attempting to woo west with COVID-19 tracking software. *Sky News*, April 4. https://news.sky.com/story/coronavirus-nso-group-attempting-to-woo-west-with-covid-19-tracking-software-11966961

McDonald, S. (2020). The Digital Response to the Outbreak of COVID-19. *Centre for International Governance Innovation*, March 30. https://www.cigionline.org/articles/digital-response-outbreak-covid-19

Morozov, E. (2013). *To save everything, Click here: Technology, solutionism, and the Urge to Fix Problems that Don't exist*. Allen Lane.

Mosendz, P., & Melin, A. (2020). Bosses are panic-buying spy software to keep tabs on remote workers. *Los Angeles Times*, March 27. https://www.latimes.com/business/technology/story/2020-03-27/coronavirus-work-from-home-privacy

Mozur, P. (2017). In urban China, cash is rapidly becoming obsolete. *New York Times*, July 16. https://www.nytimes.com/2017/07/16/business/china-cash-smartphone-payments.html

Narayanan, A., & Shmatikov, V. (2010). Privacy and security: Myths and fallacies of 'personally identifiable information'. *Communications of the ACM*, *53*(6), 24–26. https://doi.org/10.1145/1743546.1743558

NBC News. (2020). Controversial tech company pitches facial recognition to track COVID-19. April 28. https://www.nbcnews.com/now/video/controversial-tech-company-pitches-facial-recognition-to-track-covid-19-82638917537

Nellis, S. (2020). As fever checks become the norm in coronavirus era, demand for thermal cameras soars. *Reuters*, April 9. https://www.reuters.com/article/us-health-coronavirus-thermal-cameras-fo/as-fever-checks-become-the-norm-in-coronavirus-era-demand-for-thermal-cameras-soars-idUSKCN21R2SF

Nielsen, M. (2020). Privacy issues arise as governments track virus. *EU Observer*, March 23. https://euobserver.com/coronavirus/147828

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines reinforce Racism*. New York University Press.

O'Brien, C. (2020). HSE Covid-19 tracing app data will be stored on individual devices. *Irish Times*, April 29. https://www.irishtimes.com/business/technology/hse-covid-19-tracing-app-data-will-be-stored-on-individual-devices-1.4240304

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Patriquin, M. (2020). Montreal computer scientists expect to launch contact-tracing app in less than a week. *The Logic*, April 9. https://thelogic.co/news/montreal-computer-scientists-expect-to-launch-contact-tracing-app-in-less-than-a-week/

Patton, L. (2020). Oh really? Our data is secure in government hands? *The Mandarin*, April 23. https://www.themandarin.com.au/131542-oh-really-harry-our-data-is-secure-in-governments-hands/

Paul, K., Menn, J., & Dave, P. (2020). In coronavirus fight, oft-criticized Facebook data aids U.S. cities, states. *Reuters*, April 2. https://www.reuters.com/article/health-coronavirus-facebook-location/in-coronavirus-fight-oft-criticized-facebook-data-aids-u-s-cities-states-idUSKBN21K3BJ

Pew Research. (2019). Mobile fact sheet. June 12. https://www.pewresearch.org/internet/fact-sheet/mobile/

Pollina, E., & Busvine, D. (2020). European mobile operators share data for coronavirus fight. March 18. https://www.reuters.com/article/us-health-coronavirus-europe-telecoms/european-mobile-operators-share-data-for-coronavirus-fight-idUSKBN2152C2

Proctor, K., & Devlin, H. (2020). Coronavirus UK: health passports 'possible in months'. *The Guardian*, May 4. https://www.theguardian.com/politics/2020/may/03/coronavirus-health-passports-for-uk-possible-in-months

Reuters. (2020). Emirati police deploy smart tech in coronavirus fight. *Reuters*, April 24. https://www.reuters.com/article/us-health-coronavirus-emirates-smart-hel/emirati-police-deploy-smart-tech-in-coronavirus-fight-idUSKCN2260YJ

Sadowski, J. (2020). The Authoritarian Trade-Off: Exchanging privacy rights for public health is a false compromise. *Real Life Magazine*, April 13. https://reallifemag.com/the-authoritarian-trade-off/

Schectman, J., Bing, C., & Stubbs, J. (2020). Cyber-intel firms pitch governments on spy tools to trace coronavirus. *Reuters*, April 28. https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1

Schwartz, A., & Crocker, A. (2020). Governments haven't shown location surveillance would help contain COVID-19. *Electronic Frontier Foundation*, March 23. https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19

Singer, N., & Sang-Hun, C. (2020). As Coronavirus Surveillance Escalates, Personal Privacy Plummets. *New York Times*, March 23. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

Sircar, S., & Sachdev, V. (2020). Not Just Red Zones, New Rules Make Aarogya Setu Mandatory For All. *The Quint*, May 2. https://www.thequint.com/tech-and-auto/aarogya-setu-app-mandatory-for-containment-zone-red-zone-orange-zone-all-employees

Stanley, J. (2020). How to Think About the Right to Privacy and Using Location Data to Fight COVID-19. *Just Security*, March 30. https://www.justsecurity.org/69444/how-to-think-about-the-right-to-privacy-and-using-location-data-to-fight-covid-19/

Stanley, J., & Granick, J. S. (2020). The limits of location tracking in an epidemic. *ACLU*. April 8. https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf

Stokel-Walker, C. (2020). Can mobile contact-tracing apps help lift lockdown? *BBC Future*, April 16. https://www.bbc.com/future/article/20200415-covid-19-could-bluetooth-contact-tracing-end-lockdown-early

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data and Society*, *4*(2), 1–14. July–December. https://doi.org/10.1177/2053951717736335

Taylor, L. (2020). Discussion comments, Webinar: Data, Ethics and the Covid-19 crisis. April 23. https://mooreinstitute.ie/2020/04/24/video-of-the-covid-19-response-webinar-data-ethics-and-the-covid-19-crisis/

Timberg, C., & Harwell, D. (2020). Government efforts to track virus through phone location data complicated by privacy concerns. *Washington Post*, March 19. https://www.washingtonpost.com/technology/2020/03/19/privacy-coronavirus-phone-data/

Tony Blair Institute for Global Change. (2020). A Price Worth Paying: Tech, Privacy and the Fight Against Covid-19. April 24. https://institute.global/policy/price-worth-paying-tech-privacy-and-fight-against-covid-19

Url, S. (2020). Drones take Italians' temperature and issue fines. *Arab News*, April 10. https://www.arabnews.com/node/1656576/world

Vaughan, A. (2020). There are many reasons why covid-19 contact-tracing apps may not work. *New Scientist*, April 17. https://www.newscientist.com/article/2241041-there-are-many-reasons-why-covid-19-contact-tracing-apps-may-not-work/

Weaver, M. (2020). Don't coerce public over contact-tracing app, say campaigners. *The Guardian*, April 26. https://www.theguardian.com/law/2020/apr/26/dont-coerce-public-over-coronavirus-contract-tracing-app-say-campaigners

Wodinsky, S. (2020). Experian Is Tracking the People Most Likely to Get Screwed Over by Coronavirus. *Gizmodo*, April 15. https://gizmodo.com/experian-is-tracking-the-people-most-likely-to-get-scre-1842843363

Zuboff, S. (2019). *The Age of surveillance capitalism: The Fight for the future at the New Frontier of power*. Profile Books.