Using digital technologies to tackle the spread of the coronavirus: Panacea or folly?

Rob Kitchin

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

rob.kitchin@mu.ie

The Programmable City Working Paper 44

http://progcity.maynoothuniversity.ie/

21 April 2020

Abstract

Digital technology solutions for contact tracing, quarantine enforcement (digital fences) and movement permission (digital leashes), and social distancing/movement monitoring have been proposed and rolled-out to aid the containment and delay phases of the coronavirus and mitigate against second and third waves of infections. In this essay, I examine numerous examples of deployed and planned technology solutions from around the world, assess their technical and practical feasibility and potential to make an impact, and explore the dangers of tech-led approaches vis-a-vis civil liberties, citizenship, and surveillance capitalism. I make the case that the proffered solutions for contact tracing and quarantining and movement permissions are unlikely to be effective and pose a number of troubling consequences, wherein the supposed benefits will not outweigh potential negative costs. If these concerns are to be ignored and the technologies deployed, I argue that they need to be accompanied by mass testing and certification, and require careful and transparent use for public health only, utilizing a privacy-by-design approach with an expiration date, proper oversight, due processes, and data minimization that forbids data sharing, repurposing and monetization.

Keywords: coronavirus; COVID-19; surveillance; civil liberties, governmentality; citizenship, contact tracing; quarantine; movement; technological solutionism; spatial sorting; social sorting; privacy; control creep; data minimization; surveillance capitalism; ethics; data justice.

Introduction

As the coronavirus pandemic has swept the world it has been accompanied by strategies and tactics to try and combat and mitigate its effects. In the main, this has involved following a traditional public health approach 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 and proposed to augment and supplement the traditional measures within these phases, accompanied by arguments that they will improve their effectiveness through real-time mass monitoring at the individual and aggregate level, optimising population control. Indeed, a number of states were relatively quick to deploy technology-led solutions to aid their response to the conoravirus for three primary purposes: (1) quarantine enforcement/movement 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); and (3) pattern and flow modelling (knowing the distribution of the disease and its spread; how many people passed through places and whether social distancing/isolation measures are being observed).[1]

For example, citizens in some parts of China were 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.[2] The system alerts the local police when those who should be in quarantine seek to access public space or transit. Moscow authorities have rolled out a QR code app to 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.[3] Taiwan has deployed a mandatory phone-location tracking system to enforce quarantines (issuing GPS-enabled[4] phones to those that do not own one), sending text messages to those who stray beyond their lockdown range. There is a prospective fine of $33,000 for violations.[5] 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.[6] Hong Kong has issued electronic tracker wristbands to ensure compulsory home quarantine is observed.[7] And the Karnataka government in India is tracking the phones of those placed in quarantine to make sure it is maintained.[8]

Israel has repurposed its advanced digital monitoring tools normally used for counterterrorism to track the movement of phones of all coronavirus carriers in the 14 days prior to testing positive in order to trace close contacts.[9] Singapore has launched TraceTogether, a bluetooth enabled app that detects and stores the details of nearby phones to enable contact tracing.[10] In South Korea, the government is utilising surveillance camera footage, smartphone location data, and credit card purchase records to track positive cases and their contacts.[11] The Victoria government in Australia has launched a platform called Whispr to allow authorities to track the locations of confirmed cases and correspond with them via text message if they are not self-isolating, and also trace their contacts.[12] They are also planning to use military drones to 'monitor temperature, heart and respiratory rate, and identify people sneezing or coughing in outdoor and indoor spaces.'[13] 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.[14] Liechtenstein is piloting the use of biometric bracelets to monitor in real-time vital bodily metrics including skin temperature, breathing rate and heart rate of wearers, with the aim to fully deploy across all citizens within months.[15]

Other countries such as the UK,[16] Ireland,[17] New Zealand,[18] Canada[19] and France[20] are planning or have proposed the use of contact tracing technologies, principally to manage the exit from the delay phase and mitigate against a second and third wave of infections.[21] 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[22] and sponsoring hackathons.[23]

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,[24] with Google also monitoring the effects of interventionist measures across cities and regions globally.[25] 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.[26] NSO Group, the company behind Israel's contact tracing solution, have offered their services to a number of governments.[27] X-Mode, a location tracking company and the data source for Culmen International, who are mapping the virus spread for US federal agencies, is providing flow data of people's movement.[28] Unacast, a location-based data broker, is using GPS data harvested from apps installed on smartphones to determine if social distancing is taking place,[29] 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.[30]

Palantir, a secretive data analytics company with a reputation for working with police and intelligence agencies,[31] 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.[32] 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.[33] 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.[34] 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.[35]

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. But such a perspective raises pressing questions, such as: are these technologies legitimately deployed? Do, or will, they effectively limit the spread of the virus? Indeed, the repurposing of existing, and the development of new, technologies to aid the battle against the coronavirus raises a whole series of questions concerning: their feasibility, validity, utility and effectiveness; their immediate and downstream consequences with respect to civil liberties and citizenship; and the creation of market opportunities for technology companies and the legitimation of surveillance capitalism (see Table 1 for summary of issues). These questions deserve careful consideration. Building on my research on the ethics of digital technologies[36] and the work of other commentators who have turned their attention to the issue (see

endnotes), my aim in this paper is to assess the technical and practical feasibility of deployed and proposed tech solutions to delay and contain the spread of the coronavirus, and critically appraise their wider implications.

Table 1: Issues arising from the use of digital technologies for tackling the spread of the coronavirus

Technical/practical	Civil liberties and citizenship	Surveillance capitalism
• Technological solutionism • Robust, domain-informed design • Pilot testing and quality assurance • Fit-for-purpose • Rule-set and parameters • Fragmented data sources • Data coverage and resolution • Representativeness and digital divides • Data quality, reliability and false positives • Duping and spoofing • Dependent on effective virus testing and certification • Contact tracing dependent on 60% participation; • Quarantining/movement 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

Will technology solutions work?

There is no question that the coronavirus demands far-reaching public health measures to meet the urgent challenge it poses. But are digital technologies a suitable and viable means to delay and contain the spread of the virus, flatten the curve and limit future waves of infection? Key questions overlooked in the hype to promote technology solutions are whether they are fit-for-purpose and will they produce the intended outcomes? Here, I consider these questions in detail with respect to phone-based contact tracing and quarantine enforcement (digital fences)/movement permission (digital leashes).[37]

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.[38] 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. There are a number of ways that proximity might be determined via: cell-site location information (CSLI) that records phone connections to nearby towers, GPS signals, wifi connections, and Bluetooth, or a combination of each of these.[39]

However, the problem with each of these methods is that they lack the precision and resolution required for meaningful contact tracing. 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 time of infringement is impossible. CSLI is far too coarse (half-a-mile or more) and wifi is too partial in coverage outside of densely urbanized places to be of use. GPS can have a resolution of 1 metre, but more typically it is 5 to 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.[40] Bluetooth does not calculate location, instead able to communicate with other devices up to a range of 100 feet (the proposed Apple/Google solution uses Bluetooth, enabling an exchange and recording of a crypto-code ID that subsequently can be traced).[41] However, not all phones have it turned on by default.[42] In addition, none of these technologies can determine if there is a physical wall or glass 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.[43] 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. In other words, it is not presently possible to determine meaningful proximate contacts and limit overloading the system with false positives.

The rationale for using digital fences and leashes is that they provide a robust and rapidly scalable means for individualised 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.

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).[44] 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.[45] 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.[46] Alternatively, they might decide not to share information if they are experiencing symptoms, or decide to avoid taking a test. As Teresa Scassa[47] 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?' Further, Ross Anderson has suggested that: 'The performance art people will tie a phone to a dog and let it run around the park; the Russians will use the app to run service-denial attacks and spread panic; and little Johnny will self-report symptoms to get the whole school sent home.'[48] 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.[49] Alerts are also susceptible to scamming, with police warning of bogus text messages stating that the phone owner knows somebody who has contracted the virus and providing a link for more information.[50]

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.[51] 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%.[52] There are also differentials across class and race. 29% of Americans who earn less than $30,000 per annum do not own a smartphone,[53] which makes contract tracing within this group less effective[54] 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.[55] 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 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.[56] 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.[57] It might be easier to enforce a lockdown rather than to confine people to endless periods of self-isolation because of instructions based on weak and false data. 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.[58] 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."[59]

Critical conditions

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

(1) there is a program of mass testing, with certification, to confirm that a person has the virus and if tracing or digital fencing/leashing is required;[60]

(2) the number of cases is low 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; [61] there is full compliance and adequate policing of quarantining/movement permissions.

(4) there is a firm legislative basis for deployment of technology-led solutions.[62]

Without an extensive regime of testing with certification, known documented cases to trace from will be absent. In addition, a large number of unknown 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. However, the advice being given to those contacted may have limited value if they have already contracted and recovered from the virus. 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.[63] This will lead to an enormous number of false positives.

Developers suggest that for phone-based contact tracing systems to be effective they would require 60% of the population to participate (equivalent to c.80% of smartphone owners in the UK).[64] As Wolfie Christl[65] notes, participation can be voluntarily, linked to non-essential rewards, de-facto compulsory in association with testing, or totally compulsory. In democratic countries where authoritarian measures are uncommon and lack legal basis, opt-in is the only viable, legal option without legislative change, though it might be possible to frame participation as a 'choice', wherein it is not compulsory but adoption is required to be exempt from lockdown measures.[66] Even then, it is likely to be subject to legal challenge[67] and coercion to participate is likely to be met with resistance and subversion. In Singapore, where its TraceTogether app was opt-in, only 12% of the population installed it,[68] suggesting

that gaining a 60% adoption rate elsewhere will be a challenge. Similarly, it will be difficult in non-authoritarian states to implement and enforce the use of digital fences and leases without legislative changes, new infrastructure, and strong policing with punitive penalties.

In short, the critical conditions needed for the successful deployment of technology solutions to limit the spread of the coronavirus are absent for many jurisdictions and will be difficult to achieve in practice.

Technological solutionism

Tech-based approaches to the coronavirus have been pursued without enough consideration of these technical and contextual issues. There is little evidence of rigorous pilot testing or extensive assessment before rollout. Rather, it seems there has been a rush to implement first and only then to consider assessing the appropriateness, configuration and utility of the technology. In particular, what seems to be overlooked is the need for wide-scale, systematic testing for the virus to enable tech solutions to work effectively; and, with respect to contact tracing, low numbers of cases and a transmission rate of $R<1$, and a participation rate of 60% of population. In any jurisdiction where testing is rationed, such as the UK and US, mass surveillance technology solutions are unlikely to warrant the trade-off in civil liberties for public health. Moreover, in terms of tackling second and third waves, the advice being given may be of little use for those who have already been infected and recovered, meaning they might self-isolate for no reason, impacting their livelihood which has already been badly affected by the first wave, or unnecessarily keeping key staff away from the frontline.

The development of contact tracing apps has all the hallmarks of trying to close the stable door after the horses have bolted. If there was a time for them it was at the very start of the pandemic when cases were very small in number. Even then, it may well be the case that small data, narrowly mined and curated by trained contact tracers using a proven methodology may have more utility than the open-pit mining of fragmented big data with limited representativeness. At best, tech-based contact tracing can only supplement, not replace, traditional methods due to its shortcomings. As the Ada Lovelace Institute concludes: “There is currently insufficient evidence to support the use of digital contact tracing … [t]he technical limitations, barriers to effective deployment and social impacts demand more consideration.” Quarantining and movement permissions require all citizens to have cell/smartphones and the deployment of new infrastructure, and also have social impacts that will likely make it difficult to deploy in non-authoritarian states.

In effect, what Evgeny Morozov calls technological solutionism[69] – that is, technology is seen as the only viable solution to resolve an issue, and policy is led by technology rather than vice-versa – has being actively promoted and pursued by those pushing tech-led measures. Such solutionism frames mass surveillance or tech-mediated control as the primary means to beating the disease,[70] adopting a systems-thinking, deterministic approach rather than a socio-technical view. When shortcomings are highlighted, the attitude almost seems to be: 'using the tech, even if flawed or unsuitable, is better than not using it.' This might be fine if there were no significant other consequences to their roll-out, but as I discuss in the next section, this is not the case. Indeed, the worry for civil liberties groups is precisely that the pursuit of flawed tech solutions 'will lead to investments that do little good, or are actually counterproductive', including a chilling effect on public trust and public health measures, and will invade privacy and undermine other civil liberties 'without producing commensurate benefits.'[71] It is a view shared by research and advisory bodies such as the Ada Lovelace Institute.[72]

Civil liberties, citizenship, and surveillance capitalism

Beyond technical and practical feasibility issues, the consequences of deploying these systems appear to have been little considered, or have been have been determined as 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.[73] 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, such as the Israeli example, 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.[74]

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; and that they would store nearly all data on users' phones.[75] Others have promoted the use of a decentralized approach, as with the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)[76] and Decentralized Privacy-Preserving Proximity Tracing (DP-3T)[77] initiatives. However, there is 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.[78] From these, the data could be shared with third parties.[79] 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.[80] For companies, such as Palantir, modelling 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. Then there are concerns about data security and vulnerabilities that might open up data to scrutiny, as detailed by Christian Schmidt in an overview of government coronavirus apps from around the world.[81]

In addition, there have been concerns that data could be re-identified, undoing the process of anonymization.[82] Indeed, it is well established in the big data literature that it is possible to reverse engineer anonymisation strategies by combing and combining datasets unless the data are fully de-identified.[83] In South Korea, for example, it proved relatively straightforward to re-identify early patients.[84] 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.[85] 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.[86] De-identification requires both direct identifiers and quasi-identifiers (those highly correlated with unique identifiers) to be carefully removed.[87] The extent to which this is happening, or will happen, is not clear.

The implications for privacy is worrying enough for many; however, the consequences extend to governmentality and civil liberties more generally. Contact tracing and movement monitoring are designed to rescript how we live our lives, reshaping social contact and movement.[88] They socially and spatially sort, redlining who can and cannot mix, move and access spaces and services. As Miriyam Aouragh, Helen Pritchard and Femke Snelting[89] 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.' In other words, these apps are designed to implement disciplining (nudging people to comply with social distancing for fear of the consequence of close contacts) and control (actively prescribing spatial behaviour, where there is little choice but to comply)

forms of governmentality. As the ACLU, EFF and others have pointed out, these forms of governmentality will be unevenly applied across populations, particularly given the demographics of 'essential workers' across retail, service, distribution industries and public health and the wider public sector. As noted with respect to algorithmic governance in general, this unevenness and inequity of access to and application of technology will reproduce data justice[90] issues across class, race, ethnicity and gender.[91]

In effect, smartphone infrastructure is being subject to control creep;[92] that is, its original purpose is being extended to perform surveillance and governance work. Over the past two decades, particularly post 9/11, control creep has been occurring across networked utility systems, with technologies designed to deliver specific services being enrolled into policing and security apparatus.[93] While in the present crisis control creep is occurring and being sought for the purposes of public health, the danger is that its use in such a fashion normalizes 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.[94] Certainly, the control creep that happened post 9/11 was not subsequently rolled back.[95]

With good reason, then, there are fears that the systems activated to tackle the pandemic will not be turned off after the crisis, instead becoming part of the new normal in monitoring and governing societies.[96] As Martin French and Torin Monahan[97] 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 shift the mode 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 in managing activity and movement. 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'.[98] As Snowden, Wikileaks, and numerous other investigations have shown, states have a poor record at practicing dataveillance,[99] 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 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.[100] 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.[101] 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.[102] 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'.[103]

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, the right to redress and to opt-out.[104] If one does opt-in to using a contact tracing app, should 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, do 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 in the rush to develop systems that such due process and oversight are being put in place.[105] Without them, will people be willing to participate in such schemes?

All these civil liberty concerns regarding privacy, governmentality, control creep, and legality could have negative impacts on public health initiatives.[106] In Korea and Singapore where early patients were re-identified they were publicly hounded and shamed, having a chilling effect on testing.[107] In the long-run concerns will have a detrimental impact. People will opt-out of the technology, or find ways to circumvent and subvert it, or avoid testing or seeking health care.[108] This will especially be the case for those who may not have the means and social supports from the state to stay socially isolated. Public education and voluntary measures and compliance are more effective than law enforcement approaches in tackling public health issues,[109] and any heavy-handed measures are likely to 'sour the relationship between citizens and their government when trust is of paramount importance.'[110] As a consequence, there is a danger that the technologies will have the opposite effect to that desired.

What this discussion highlights is that contact tracing and quarantining/movement restriction technologies raise fundamental questions of citizenship and the rights and entitlements of those living within a jurisdiction. These rights and entitlements clearly have to be weighed against the public health of a nation and the right to life of other citizens. However, traditional contact tracing at the very start of a pandemic when cases are small would keep the transmission rate near to zero, and implementation once the disease is well established is likely to have limited effects. Moreover, nations such as Ireland have demonstrated it is possible to reduce the transmission rate to below one and near to zero without using mass, fine-grained surveillance and digital fences/leashes. In this context, the issues raised with respect to civil liberties and citizenship cannot be simply pushed to one side for the 'greater good' of public health. Instead, there is a need to consider the extent to which technology-led approaches will deliver on their promise and the trade-offs occurring on the basis of that promise, including how these trade-offs might be to the benefit of surveillance capitalism.[111]

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.[112] 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 than record and transmit GPS coordinates, with 58 companies specialising in location tracking operating in the US alone in 2014,[113] which has since grown. In addition, telecommunication companies, social media companies such as Facebook (inc. Whatsapp and Instagram), Snapchat and Twitter, 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 coronavirus pandemic has laid it bare through the offers of these companies to share data and analytic tools to aid contact tracing and to monitor the effects of social distancing.

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'[114] of surveillance capitalism as a way of laundering their reputations.[115] Through the use of these data and services states and researchers are, in effect, normalizing the surveillance and business practices of these companies. While unintentional, they are also helping to boost their 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 coronavirus, pitching several potential new products and markets, including social distance policy enforcement.[116] No doubt some companies hope that contributing to tackling coronavirus will potentially act as a gateway to public health and other government contracts,[117] as well as to the further privatisation 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 coronavirus pandemic will cement and legitimate the practices of surveillance capitalism, which has done much to undermine civil liberties related to privacy and mainstreamed commercial social and spatial sorting and profiling. And yet, these companies expect to be praised for their interventions, as expressed by Eric Schmidt, the former CEO of Google, who believes that people should be 'a little bit grateful' for the

services provided by big tech.[118] While some of these services may be useful, they are also a double-edged sword.

What needs to happen?

To date, governments have not demonstrated they have comprehensively assessed all technical and practical issues, or considered in a meaningful way civil liberties and citizenship issues, or indeed been transparent about their plans and rationales.[119] Groups like PEPP-PT and DP-3T are open and have sought to address privacy and data security issues, though there seems less consideration of other critical conditions required for the technology to work. Rather than rush headlong into rolling out mass surveillance systems there is a need for proper, open debate on the solutions to the crisis – even if that is conducted quickly over the course of a few days, rather than not all – that includes setting out the viability and pros and cons of all potential solutions (tech/non-tech), and details all the checks/balances that would be needed with regards to each to ensure civil liberties while enabling mitigation.

Governments and companies need to set out in clear and unambiguous terms their rationale for wanting to implement and how they envisage technologies will work and deliver. This needs to include how they will address the shortcomings detailed above, how they will dovetail with an extensive regime of mass virus testing, and assess their social and legal impact. We then need to establish whether the proposed technology-led solutions to the coronavirus are really going to produce effective results beyond the more traditional social and governance measures being implemented, and whether they might have a negative, chilling effect on public health. If we believe that they will work and are necessary, then we need to determine quickly through expert review what configuration will work best for our intended ends while also considering long-term governance. Speed is obviously essential, but it is not unreasonable to be able to assemble a team and robustly assess potential options over a couple of days. The Ada Lovelace Institute (2020), for example, recommends that the UK establishes what it terms 'Group of Advisors on Technology in Emergencies' (GATE) to assess and act as gatekeepers for the deployment of technologies to tackle the coronavirus.[120]

For any tech solution that is developed, we need to insist that it is appropriate and proportionate, meeting the guidance of the Electronic Frontier Foundation, American Civil Liberties Union, and the Ada Lovelace Institute:[121]

- 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;
- data cannot be shared beyond 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.

In other words, 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 app seeks 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.

Conclusion

My aim in this paper has been to provide a relatively comprehensive overview of the technical, practical, and ethical issues of developing and deploying technology solutions to delay and containment measures for tackling the coronavirus. There is no doubt that much of the response is well-intentioned, undertaken by actors who are keen to leverage their professional skills and products to try and meaningfully contribute to limiting the effects of the disease.[122] However, 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 given as to their consequences for

civil liberties or surveillance capitalism and whether the supposed benefits outweigh any commensurate negative effects.

The analysis presented suggests that the technology solutions deployed and proposed have been oversold. Smartphone based contact tracing will be ineffectual without mass testing (not self-diagnosis) and certification, and it needed to be introduced when the number of infections were very low. Moreover, the spatial resolution is too coarse to capture proximity less than two metres, and it requires a 60% opt-in rate which is unlikely to be achieved. It is doubtful that quarantine and movement permission technology will be accepted by the populations in non-authoritarian states and the necessary scanning infrastructure would need to be put in place. And while governments and companies have sought to reassure about civil liberties, it is clear that the technology does have implications for privacy, governmentality, control creep, and citizenship, and they do reinforce the logic of surveillance capitalism.

Given this imbalance between benefits and pitfalls it seems necessary to review the use and utility of technologies already deployed and foolhardy to proceed with the use of proposed technologies until they have been more fully assessed, debated and empirically tested and proven. If they are already deployed or are to proceed regardless, then they require careful and transparent use for public health only, utilizing a rights-based and privacy-by-design approach with an expiration date, proper oversight, due processes and data minimization that forbids data sharing, repurposing and monetization, and they need to be accompanied by mass testing and certification. We should be careful as we seek to manage and mitigate the coronavirus pandemic that we do not rush into adopting technologies could cause more harm than good.

Acknowledgements

I am grateful for the feedback of Alistair Fraser, Tracey Lauriault and Sophia Maalsen on the first draft of this paper.

---

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

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

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

[4] Global Positioning System

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

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

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

[8] Agrawal, A. (2020) Karnataka govt and Mumbai Police track phones of people quarantined due to coronavirus: Report. *Medianama*, March 19th, https://www.medianama.com/2020/03/223-karnataka-phone-tracking-coronavirus/

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

[10] Singer, N. and Sang-Hun, C. (2020)

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

[12] Lane, I. (2020) From drones to phone tracking: Coronavirus crisis puts our civil liberties at risk, experts warn. *The New Daily*, March 26th. https://thenewdaily.com.au/life/tech/2020/03/26/coronavirus-surveillance-civil-liberties/

[13] Lane, I. (2020)

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

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

[16] Devlin, H. (2020) NHS developing app to trace close contacts of coronavirus carriers, *The Guardian*, 31 March, https://www.theguardian.com/uk-news/2020/mar/31/nhs-developing-app-to-trace-close-contacts-of-coronavirus-carriers

[17] Horgan-Jones, J. (2020) Coronavirus: Smartphone app to facilitate contact tracing to be rolled out, HSE says. *Irish Times*, 29 March, https://www.irishtimes.com/news/ireland/irish-news/coronavirus-smartphone-app-to-facilitate-contact-tracing-to-be-rolled-out-hse-says-1.4215036

[18] Kilgallon, S. (2020) Coronavirus: Kiwi tech firm offers up Covid-19 app to government. *Stuff*, 9 April, https://www.stuff.co.nz/technology/apps/120918665/coronavirus-kiwi-tech-firm-offers-up-covid19-app-to-government

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

[20] Untersinger, P.M., Hecketsweiler, C. and Beguin et Oliver Faye, F. (2020) L'application StopCovid retracera l'historique des relations sociales: les pistes du gouvernement pour le traçage numérique des malades. *Le Monde*, 8 April, https://www.lemonde.fr/planete/article/2020/04/08/stopcovid-l-application-sur-laquelle-travaille-le-gouvernement-pour-contrer-l-epidemie_6035927_3244.html

[21] For other examples of the tech being deployed by states to tackle the spread of the coronavirus see https://privacyinternational.org/examples/tracking-global-response-covid-19

[22] 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

[23] 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/

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

[25] https://www.google.com/covid19/mobility/

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

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

[28] Levinson, C. (2020) Phone tracking is having a moment, but gay dating app Scruff wants no part of it. *Protocol*, 6 April, https://www.protocol.com/scruff-rejects-selling-location-data

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

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

[31] McDonald, S. (2020) The Digital Response to the Outbreak of COVID-19. Centre for International Governance Innovation, March 30th. https://www.cigionline.org/articles/digital-response-outbreak-covid-19; Sadowski, J. (2020) The Authoritarian Trade-Off: Exchanging privacy rights for public health is a false compromise. *Real Life Magazine*, April 13th. https://reallifemag.com/the-authoritarian-trade-off/

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

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

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

[35] https://twitter.com/WolfieChristl/status/1246079249544630279

[36] http://www.kitchin.org/?page_id=1457

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

[38] 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

[39] Stanley, J. and Granick, J.S. (2020)
[40] Stanley, J. and Granick, J.S. (2020); Schwartz, A. and Crocker, A. (2020)
[41] In this case, all people who have been near to a person who has informed the associated public health app that they have tested positive are alerted to the fact. Sullivan, M. (2020) How Apple and Google's coronavirus-tracking technology works. *Fast Company*, 14 April, https://www.fastcompany.com/90490059/how-apple-and-googles-coronavirus-tracking-technology-works
[42] Stanley, J. and Granick, J.S. (2020)
[43] Kelion, L. (2020)
[44] Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Sage, London.
[45] McDonald, S. (2020)
[46] Stanley, J. and Granick, J.S. (2020)
[47] Patriquin, M. (2020)
[48] Angwin, J. (2020)
[49] Angwin, J. (2020)
[50] Tyree, E. (2020) 'DO NOT click the link'; Police warn of scam COVID-19 text messages. *ABC 13 News*, 16 April, https://wset.com/news/coronavirus/do-not-click-the-link-police-warn-of-scam-covid-19-text-messages
[51] Stanley, J. (2020) How to Think About the Right to Privacy and Using Location Data to Fight COVID-19. *Just Security*, 30 March, https://www.justsecurity.org/69444/how-to-think-about-the-right-to-privacy-and-using-location-data-to-fight-covid-19/
[52] Pew Research (2019) Mobile fact sheet. 12 June. https://www.pewresearch.org/internet/fact-sheet/mobile/
[53] Pew Research (2019)
[54] Schwartz, A. and Crocker, A. (2020) Governments haven't shown location surveillance would help contain COVID-19, *Electronic Frontier Foundation*, 23 March, https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19
[55] Ems, L. (2015) Exploring ethnographic techniques for ICT non-use research: An Amish case study. *First Monday* 20(11). https://journals.uic.edu/ojs/index.php/fm/article/view/6312/5139
[56] Angwin, J. (2020)
[57] Angwin, J. (2020)
[58] Linder, R. (2020) Quarantined After Waving at Coronavirus Patient: How Accurate Is Israel's 'Terrorist-tracking' Tech? *Haaretz*, 22 March, https://www.haaretz.com/israel-news/.premium-isolated-after-waving-at-corona-patient-is-israeli-phone-tracking-tech-accurate-1.8698946
[59] Stanley, J. and Granick, J.S. (2020); Also see McDonald (2020)
[60] 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
[61] Stokel-Walker, C. (2020); Kelion, L. (2020)
[62] Ada Lovelace Institute (2020)
[63] Kelion, L. (2020) Coronavirus: NHS contact tracing app to target 80% of smartphone users. *BBC News*, 16 April, https://www.bbc.com/news/technology-52294896
[64] Stokel-Walker, C. (2020); Kelion, L. (2020)
[65] https://twitter.com/WolfieChristl/status/1245701670824292354
[66] https://twitter.com/WolfieChristl/status/1249652821705871366
[67] Stanley (2020); Stokel-Walker, C. (2020)
[68] Kelion, L. (2020)
[69] Morozov, E. (2013) *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems That Don't Exist*. New York: Allen Lane.

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

[71] Stanley, J. and Granick, J.S. (2020)

[72] Ada Lovelace Institute (2020)

[73] Schwartz, A. and Crocker, A. (2020); Stanley, J. and Granick, J.S. (2020); Angwin, J. (2020)

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

[75] Angwin, J. (2020)

[76] https://www.pepp-pt.org/

[77] https://github.com/DP-3T/documents

[78] Angwin, J. (2020)

[79] Patriquin, M. (2020)

[80] Angwin, J. (2020)

[81] https://twitter.com/PiracyByDesign/status/1241380421436407808

[82] See https://twitter.com/ashk4n/status/1250071326372638736 for an example of how this might be done.

[83] Narayanan, A. and Shmatikov, V. (2010) Privacy and security: myths and fallacies of 'personally identifiable information'. *Communications of the ACM* 53(6): 24-26; de Montjoye, Y.A., Hidalgo, C.A., Verleysen, M. and Blondel, V.D. (2013) Unique in the Crowd: The privacy bounds of human mobility. *Nature, Scientific Reports* 3, article 1376: 1-5 http://www.nature.com/articles/srep01376.pdf; Ducklin, P. (2015) The Big Data picture - just how anonymous are 'anonymous' records? *Naked Security*, 12 February. http://nakedsecurity.sophos.com/2015/02/12/the-big-data-picture-just-how-anonymous-are-anonymous-records/

[84] Singer, N. and Sang-Hun, C. (2020)

[85] Singer, N. and Sang-Hun, C. (2020)

[86] https://chp-dashboard.geodata.gov.hk/covid-19/en.html

[87] Cavoukian, A. and Castro, D. (2014) *Big Data and Innovation, Setting the Record Straight: De-identification Does Work*. Information and Privacy Commissioner Ontario, Canada. www2.itif.org/2014-big-data-deidentification.pdf

[88] Aouragh, M., Pritchard, H. and Snelting, F. (2020)

[89] Aouragh, M., Pritchard, H. and Snelting, F. (2020)

[90] Dencik, L., Hintz, A. and Cable, J. (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society* 3(2): 1-12; Taylor, L. (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data and Society* 4(2), July–Dec: 1–14

[91] Benjamin, R. (2019) *Race After Technology*. Polity Books, Cambridge; Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St Martin's Press; Noble, S.U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

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

[93] Kitchin, R. and Dodge, M. (2011) *Code/Space: Software and Everyday Life*. Cambridge: MIT Press;

[94] Sadowski, J. (2020)

[95] McDonald (2020); Sadowski, J. (2020)

[96] Sadowski, J. (2020); Stanley, J. and Granick, J.S. (2020)

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

[98] Sadowski, J. (2020)

[99] Lyon D. (2015) *Surveillance After Snowden*. Cambridge: Polity Press.

[100] Liang, F., Das, V., Kostyuk, N. and 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; Lee, C.S. (2019) Datafication, dataveillance, and the social credit system as China's new normal. *Online Information Review* 43(6): 952-970; Keegan, M. (2019) Big Brother is watching: Chinese city with 2.6m cameras is the world's most heavily surveilled. *The Guardian*, Dec 2nd, https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled

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

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

[103] Ilyushina, M. (2020)

[104] McDonald, S. (2020)

[105] McDonald, S. (2020)

[106] Ada Lovelace Institute (2020)

[107] Singer, N. and Sang-Hun, C. (2020)

[108] Schwartz, A. and Crocker, A. (2020)

[109] Stanley, J. and Granick, J.S. (2020)

[110] Schwartz, A. and Crocker, A. (2020)

[111] Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. Profile Books, New York.

[112] Kitchin, R. (2014)

[113] Angwin, J. (2014) *Dragnet Nation*. St Martin's Press, New York

[114] https://twitter.com/WolfieChristl/status/1242956802930683913

[115] McDonald, S. (2020); Stanley, J. (2020)

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

[117] Sadowski, J. (2020)

[118] Schleifer, T. (2020) Google's former CEO hopes the coronavirus makes people more "grateful" for Big Tech. *Vox: Recode*, 14 April, https://www.vox.com/recode/2020/4/14/21221141/coronavirus-eric-schmidt-google-big-tech-grateful

[119] Schwartz, A. and Crocker, A. (2020)

[120] Ada Lovelace Institute (2020)

[121] Ada Lovelace Institute (2020); Guarglia, M. and Schwartz, A. (2020); Stanley (2020)

[122] McDonald, S. (2020)