ETHICS, AI, MASS DATA AND PANDEMIC CHALLENGES: RESPONSIBLE DATA USE AND INFRASTRUCTURE APPLICATION FOR SURVEILLANCE AND PRE-EMPTIVE TRACING POST-CRISIS

Mark Findlay, Jia Yuan Loke, Nydia Remolina, Benjamin Tham[*] [**]

SMU Centre for AI & Data Governance Research Paper No. 2020/02

ABSTRACT

As the COVID-19 health pandemic rages governments and private companies across the globe are utilising AI-assisted surveillance, reporting, mapping and tracing technologies with the intention of slowing the spread of the virus. These technologies have capacity to amass personal data and share for community control and citizen safety motivations that empower state agencies and inveigle citizen co-operation which could only be imagined outside such times of real and present danger. While not cavilling with the short-term necessity for these technologies and the data they control, process and share in the health regulation mission, this paper argues that this infrastructure application for surveillance have serious ethical and regulatory implications in the medium and long term in relation to individual dignity, civil liberties, transparency, data aggregation, explainability and other governance challenges. To conduct this analysis, the paper presents the Singapore and China case studies, and offers a comparative description based on the many more initiatives implemented worldwide in order to understand the purpose, goal and risk of these infrastructures. The analysis looks at data protection and citizen integrity and reflects on other surveillance methods outside the health context, such as initiatives implemented in the financial sector, where similar challenges have arisen.

[*] Mark Findlay is a Professor of Law at Singapore Management University and Director of the SMU Centre for AI and Data Governance. Jia Yuan Loke, Nydia Remolina and Benjamin Tham are Research Associates at the SMU Centre for AI and Data Governance

[**] This research is supported by the National Research Foundation, Singapore under its Emerging Areas Research Projects (EARP) Funding Initiative. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

TABLE OF CONTENTS

INTRODUCTION 3
I. THE COVID-19 CRISIS CONTEXT 6
II. A SINGAPORE CASE-STUDY 9
1. Stay-Home Notice 10
a. Ensuring compliance with a 14-day Stay-Home Notice: Legislative framework 11
b. Surveillance capacities 13
2. TraceTogether App 16
3. Whether the data procured through MOM monitoring complies with personal data protection guidelines in Singapore 17
III. THE PEOPLE'S REPUBLIC OF CHINA ("THE PRC") CASE STUDY 18
1. Legislative backdrop 18
a. Power to implement pre-emptive tracing methods and to utilise both state and non-state resources/machinery to do so 19
2. Some technology-driven applications for surveillance 21
a. One QR code for every stop/station, one QR code for every car/carriage ("一站一码，一车一码") 21
b. Smart doorbells ("爱心门铃") 21
IV. COMPARATIVE GLOBAL RESPONSES 23
1. Clarifying contact tracing 24
a. Tracing 24
2. Maintaining quarantines 27
a. Quarantine containment 28
V. ETHICAL CHALLENGES 29
1. Public interest versus individual rights 32
2. Individual dignity 34
3. Transparency 36
4. Avoiding Biases 37
5. Data aggregation 39
6. Expiration 40
7. Explainability 40
8. Anxiety Governance 41
VI. SIMILAR USE CASES – THE FINANCIAL SECTOR APPROACH TO DATA-DRIVEN SURVEILLANCE 42
1. Regtech - Anti-money laundering, know your customer and tracing fraudulent transactions 42
2. Suptech- Misconduct and Market Surveillance by Financial Regulators 45
CONCLUSION 46

INTRODUCTION

As the COVID-19 health pandemic rages governments and private companies across the globe are utilising AI-assisted[1] surveillance, reporting, mapping and tracing technologies with the intention of slowing the spread of the virus. These technologies have capacity to amass personal data and share data sources for community control and citizen safety motivations that empower state agencies and persuade citizen co-operation which could only be imagined outside such times of real and present danger. Concern is growing about the potential for these technologies and resultant data sharing to negatively impact civil rights,[2] invade personal privacy,[3] undermine citizen dignity through expansive data matching and provide opportunities for data use well beyond the brief of virus mitigation.[4] While not cavilling with the short-term necessity for these technologies and the data they control, process and share in the health regulation mission, this paper asks three consequential questions:

1. Are there common control objectives that can be identified in the manner and application of these technologies in different geopolitical contexts, and if so how can their appropriate achievement be monitored?[5]

2. Are the objectives for these technologies clear, causally justified in control outcome terms and contained, recognising that the technologies themselves may differ widely in data management styles?[6]

---

[1] It may be argued that Bluetooth and GPS are not AI in its more limited iterations. For the purposes of this paper both these communication pathways are primarily activated through smart-phone technology which is quite clearly AI dependent insofar as algorithms essentially motivate the applications which make the device multi-functional.

[2] "Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights", *Amnesty International* (2 April 2020) <https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf> (accessed 6 April 2020)
"Human Rights Dimensions of COVID-19 Response", *Human Rights Watch* (19 March 2020) <https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response> (accessed6 April 2020)

[3] Albert Gidari, "*Op-Ed: How location history can help contain COVID-19 while protecting privacy*, A guest post by Stanford Law School's Center for Internet and Society's Director of Privacy", *Risky.biz* (27 March 2020), <https://risky.biz/gidarioped/> (accessed 6 April 2020)
"Statement on the processing of personal data in the context of the COVID-19 outbreak", European Data Protection Board (20 March 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en> (accessed 7 April 2020)

[4] Matthew Guariglia and Adam Schwartz, "Protecting Civil Liberties During a Public Health Crisis", *Electronic Frontier Foundation*(10 March 2020) <https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis> (accssed April 2 2020)

[5] There is no empirical monitoring constructed or carried out in this analysis, and although such was not intended in this work, the case-studies are replete with reference to stated purposes, and regular consideration is given to whether these seem to be achieved or exceeded.

[6] Our analysis of the technology is agnostic in the sense that regardless of the use of a particular technology, there are always ethical challenges, and as such the paper confines its critique to the implemention of tracing, tracking and surveillance programmes that involve personal data management.

3. What are the medium term[7] ethical challenges posed by the proliferation of these technologies and their data management, after the virus danger has abated and control has reverted to more conventional medical interventions and strategies?

Before summarising the intended development of our argument, the importance of a timely analysis regarding surveillance and data use in crisis contexts is revealed by reflecting on in each of these questions as they concern objectives and outcomes.[8] If there are particular objectives that promote citizen tracking for instance, have these been well enunciated so that limits on ancillary data use can be affected without diluting the short-term legitimate control motivations? Are citizen data subjects aware of the limited purposes for data collection and shared analysis? Is there, consistent with so many ethical codes for the use of AI-assisted data collection and usage, regulatory mechanisms in place that guarantee transparency, accountability and expunging?

Consistent with the medium-term data-governance aspirations for the paper, it is essential to refine down the extensions of pre-existing surveillance authority and the crisis-led differences in novel technologies and data sharing to at least describe how these technologies are employed by states and private sector entities world-wide. From a description of the surveillance and tracking terrain, and the nature of mass data accumulation and shared usage against limited crisis purposes, it is easier to be specific about the temptations to convert crisis monitoring into permanent social surveillance and the dangers that the private/public sector alliances pose to these purposes. In terms of the general ethical challenges represented in such eventualities, we want to particularise from broad concerns of privacy and data protection (which in Asia may be thought of as second order data-integrity measures), to more expressly targeted issues of freedom of movement and association (which have been heavily contested in the enforcement of the Singapore circuit breaker through grassroots resistance),[9] confidence in data use for data purpose, trust in data sharing, and overall fairness. The development of this analysis is assisted if it grows from an expressed interrogation of crisis-led purpose and objectives

A first step in answering any enquiry into purpose/objectives is to categorise tracing styles. Should they be comparatively understood in terms of method, volition of participation, mandatory application, location, application or goal? While not exhaustively comparing the immediate and projected objectives inherent and declared in each technology and the data they generate and share against voluntary participation, for instance, we do indicate what intentions produce what outcomes and how these may translate into consequences which could not be so easily tolerated outside crisis contingencies.

---

[7] Ideas on defined phasing in the pandemic down surge are at this stage a political question. There will be no clear end to the pandemic agreed by science for some time, but there will be political determinations as to the end of crisis measures. Therefore, we will talk about excessive data use during the crisis and as it winds down (so defined by a downgrading 0f crisis data usage) and in the long term.

[8] In so doing this is not to say that consistency of objective and outcome is the primary challenge to be addressed in data usage. Objective consistency is offered only as on simple and non-contentious framework for limiting extended and ungoverned data usage ongoing.

[9] "28-day circuit breaker may not be enough if Singaporeans don't play their part, says Masagos", *Channel News Asia* (16 April 2020) <https://www.channelnewsasia.com/news/singapore/covid-19-circuit-breaker-mask-enforcement-masagos-coronavirus-12649274> (accssed 22 April 2020)

In terms of the latter option some examples currently include:

1. **Identifying** close contacts after someone tests positive for the virus. Especially in countries that reacted swiftly like Singapore, Taiwan, and Hong Kong, this has been a dominant process (contact tracing).[10]

2. Needing to **monito**r people who have been asked to stay home (e.g. close contacts, people returning from overseas, then the general population).[11]

3. Pre-emptive **tracing** (e.g. making people register before they enter venues). This is considered a significant initiative prior to lifting lock-down restrictions and "releasing" people from isolation.

4. **Mass mapping** and movement tracing in order to see where infected individuals have travelled and to inform people in the vicinity of such movement.[12]

5. **Demographic quarantining –** isolating sectors of the population and preventing external movement and association, while at the same time anticipating internal infection due to the inapplicability of social distancing.

Each of these surveillance styles will be discussed in two analytical contexts. The first will be to identify in more detailed case-studies of Singapore and the PRC, the different approaches adopted in tracing, tracking and surveillance, and return to the authorisation for these strategies. The second is a brief overview of trends in other jurisdictions, in an attempt to link technologies, to control outputs and suggest some of the consequences for data integrity and surveillance containment.

In some respects, similar goals can be accomplished with different methods, such as identifying close contacts relying on verbal information from the patient or examining CCTV footage. Also, different goals may rely on the same method. An example is the use of phone-based location tracking to achieve all four goals above. It is difficult to challenge the legitimacy of these goals in times of emergency. It is the methods for their achievement, the mass data they make available to scores of interrelated databases, and the ethical challenges and data integrity implications of these methods and data-driven initiatives during and beyond the life of the crisis that will exercise the analytical interest of the paper's concluding section.[13]

In the argument and analysis to follow, there are two levels at least at which goals can be utilised both as an analytical tool and a potential regulatory qualifier post crisis. The first is 'expressed' 'extant' goals, meaning the immediate stated purpose in the context of the health crisis. This more apparent and limited aspirational range is recognised in the

[10] See Appendix A. Table 1. Tracing and surveillance initiatives in different jurisdictions.
[11] Singapore and China case-studies below
[12] Singapore and China case-studies below.
[13] In future iterations of this work it is intended to offer policy recommendations to reduce the negative impacts on privacy, civil rights, data integrity, and public trust.

debate around whether tracing is surveillance in the narrow sense.[14] But equally important is 'potential' 'expansive' goals achievable mainly in the medium-term surveillance. From what is a fairly formative and evolving perspective in the development and use of these technologies we can only speculate on potential risks in the extended or permanent use and applications of personal data so produced. That said, crisis-led surveillance is not a novel phenomenon. What makes it different on this occasion is the sophistication and reach of the technology so far employed, largely reliant on an almost total smart-phone coverage in countries most-actively employing these technologies. From such a technological armoury, the state's potential to surveil the citizen ongoing and to mass share data (personal/aggregated) far beyond crisis exigencies is the product of big data and a new disposition from private platforms to cooperate with each other and share resources and information with the state.

This paper commences with a detailed descriptive case-study of the Singapore response, focusing on legal regulatory empowerment. The reason for this is that Singapore has been active, experimental and early in the surveillance and tracking response. Looking at law as a first point of regulatory reference helps understand how the state intends citizen compliance, and how it envisages the limitations of its powers. In contrast, there follows a brief overview of the response in the PRC not so consciously justified through law, elaborated on by some limited local commentary. China is often viewed as the most intrusive data logging jurisdiction in many aspects of state/citizen engagement and there has been recent concern expressed within and outside China about how an authoritarian one-party state may adapt the crisis to more permanent scenarios of social engineering.[15] These case studies are followed by a comparative snapshot of other responses in different geopolitical locations, technological climates, political cultures and contexts of the crisis. Expanding the comparative description is intended to offer a more thematic understanding of purpose, goal and risk. Obviously as the crisis evolves, this work will require expansion and elaboration. The remaining body of the paper explores challenges posed by these technological and data developments. The analysis looks at privacy, data protection and citizen integrity and reflects on other surveillance methods, outside the health context, where similar challenges have arisen. In its developed form a later version of this paper will speculate on and offer suggestions regarding regulatory responses when faced with extended surveillance, tracking/tracing, public/private provider data sharing and any breakdown in personal data firewalls, or otherwise conventional aggregated data constraints.

I. THE COVID-19 CRISIS CONTEXT

COVID-19 is the disease caused by the virus SARS-CoV-2 (hereinafter referred to as "the Virus"). According to current scientific evidence, the Virus is transmitted between

[14] "Contact-tracing apps raise surveillance fears", *Financial Times* (21 April 2020) <https://www.ft.com/content/005ab1a8-1691-4e7b-8e10-0d3d2614a276> (accessed XXYY)

[15] Lily Kuo, "The new normal': China's excessive coronavirus public monitoring could be here to stay", *The Guardian* (9 March 2020)https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay (accessed XXYY)

people through respiratory droplets and contact routes.[16] Therefore, transmission of [the Virus] can occur by direct contact with infected people and indirect contact with surfaces in the immediate environment or with objects used on the infected person (e.g. stethoscope or thermometer)."[17]

The Virus is easily transmitted and, indeed, infection rates have proven to be very high. As of early April, the total number of confirmed cases of COVID-19 for the United States, Spain and Germany doubles approximately every 2.5 days since their 100th confirmed case of COVID-19. In Turkey, the total number of confirmed cases doubles in less than 2 days since its 100th confirmed case.[18]

The high infection rates severely threaten national healthcare institutions. As Associate Professor Nahid Bhadelia, an infectious diseases expert at the Boston University School of Medicine observed: "No matter what, [the Virus] was going to test the resilience of even the most well-equipped health systems."[19] This happens in several ways. For example, insufficient COVID-19 testing kits, isolation rooms, ICU beds, trained medical professionals, vital equipment (such as personal protection equipment and ECMO[20]s), etc, to deal with the growing number of COVID-19 patients due to the high infection rates.
Resulting from the high infection rates, it is seen as imperative by most if not all governments to adopt measures to slow down the infection rate in order to ensure that national healthcare institutions do not become overwhelmed. This is otherwise known as "flattening the curve".[21]

People infected with the Virus who are unable to be isolated and/or receive medical treatment risk spreading the Virus to others, leading to increased community spread[22] of the Virus.[23] This in turn may see the exponential spread of the Virus if the number of

[16] The WHO defines droplet transmission as such: "Droplet transmission occurs when a person is in close contact (within 1m) with someone who has respiratory symptoms (e.g. coughing or sneezing,) and is therefore at risk of having his/her mucosae (mouth and nose) or conjunctiva (eyes) exposed to potentially infective respiratory droplets. (See fn 17)
[17] "Modes of transmission of virus causing COVID-19: implications for IPC precaution recommendations", *World Health Organization* (29 March 2020) <http://www.who.int/news-room/commentaries/detail/modes-of-transmission-of-virus-causing-covid-19-implications-for-ipc-precaution-recommendations> (accessed 31 March 2020)
[18] "Total confirmed COVID-19 cases: how rapidly are they increasing?", *Our World in Data* <http://ourworldindata.org/grapher/covid-confirmed-cases-since-100th-case> (accessed 31 March 2020)
[19] Ed Yong, "How the Pandemic will End", *The Atlantic* (25 March 2020) <http://www.theatlantic.com/health/archive/2020/03/how-will-coronavirus-end/608719/ (accessed 31 March 2020)
[20] Extracorporeal membrane oxygenation, a medical device which is used to treat severely ill Covid-19 patients
[21] "Boris Johnson's address to the nation in full", *The Guardian* (23 March 2020) <http://www.theguardian.com/uk-news/2020/mar/23/boris-johnsons-address-to-the-nation-in-full> (accessed 31 March 2020)
[22] "How COVID-19 Spreads", *Centres for Disease Control and Prevention* <http://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/how-covid-spreads.html> (accessed 31 March 2020)
[23] Bo Gu, "For one family, neither treatment nor closure in virus-hit Wuhan", Al Jazeera (17 February 2020) <https://www.aljazeera.com/news/2020/02/coronavirus-outbreak-treatment-closure-wuhan-200217103130283.html> (accessed 30 March 2020)

cases were to double every three days or less.[24] The exponential spread of the Virus may become further compounded if and when medical professionals themselves become infected due to a shortage of personal protection equipment, being overworked, etc.

As Dr Drew Harris, a population health analyst at Thomas Jefferson University added:

> The ideal goal in fighting an epidemic or pandemic is to completely halt the spread. But merely slowing it — mitigation — is critical. This reduces the number of cases that are active at any given time, which in turn gives doctors, hospitals, police, schools and vaccine-manufacturers time to prepare and respond, without becoming overwhelmed… Slowing and spreading out the tidal wave of cases will save lives. Flattening the curve keeps society going.[25]

To slow the spread of the Virus in order to flatten the curve, "[t]he only hope we have is to lower the reproduction number [of the Virus]. And the only way to do so before a vaccine is produced is to contact trace with testing, find infected cases and isolate them."[26] Such measures reduce the contact rate between infected and susceptible people.

To act before the vaccine or other eradication alternatives are found and massively circulated, much government policy deems it also necessary to take pre-emptive measures to similarly reduce the contact rate between susceptible people and non-susceptible people, recognising susceptible people may also be carriers of the Virus. Since carriers of the virus may be asymptomatic[27] and the Virus has an incubation period[28] of 14 days, isolating susceptible people is therefore also imperative to err on the side of caution.[29]

In the control scenario susceptible people are referred to as those who are at risk of being exposed to infection carriers. This includes, for example:

> People exposed to infected people due to natural proximity (save for medical professionals): For example, people who live in the same house as an infected person
> People returning from other countries
> People who are under medical leave for displaying respiratory symptoms.

Different countries adopt different measures to flatten the curve. Two such measures that involve data collection/use are:

---

[24] Harry Stevens, "Why outbreaks like coronoavirus spread exponentially, and how to 'flatten the curve'", *The Washington Post* (14 March 2020) <http://www.washingtonpost.com/graphics/2020/world/corona-simulator/> (accessed 30 March 2020)

[25] Siobhan Roberts, "Flattening the Coronavirus Curve", *The New York Times* (27 March 2020) <http://www.nytimes.com/article/flatten-curve-coronavirus.html> (accessed 31 March 2020)

[26] Siobhan Roberts, "The Exponential Power of Now", *The New York Times* (13 March 2020) <http://www.nytimes.com/2020/03/13/science/coronavirus-math-mitigation-distancing.html> (accessed 31 March 2020)

[27] "Asymptomatic coronavirus carriers: How contagious are they?", *The Straits Times* (31 March 2020) <http://www.straitstimes.com/world/united-states/asymptomatic-coronavirus-carriers-how-contagious-are-they> (accessed 31 March 2020)

[28] Incubation period refers to the time between exposure to the virus and the appearance of the first symptoms

[29] Ministry of Health, Singapore website <http://www.moh.gov.sg/covid-19/faqs> (accessed 30 March 2020)

> Ensuring susceptible people who are subjected to quasi-quarantine measures[30] adhere to them strictly: Data collection/use is involved as such measures generally involves the monitoring of susceptible people under quasi-quarantine measures.
>
> Pre-emptive tracing methods: Data collection/use is involved as such methods generally involve the tracking of people whom non-susceptible people may come into contact with during their daily activities.

Once a non-susceptible person becomes infected with the Virus, the relevant authorities will be able to utilise the data obtained from the respective pre-emptive tracing method to "quickly identify other users he has been in close contact with, allowing for easier identification of potential cases and helping curb the spread of the virus."[31]

One of the ways which the discussion can contribute to the literature is by highlighting the harms of governments building surveillance infrastructures to combat COVID-19 or adapting pre-existing technological potential, which then remain around for purposes other than COVID-19 after the pandemic is over. One such example (albeit not in relation to a pandemic) would be that of the 9/11 terrorist attack where the US government created "new surveillance infrastructure [that] gave more power to the very institutions whose failure created the crisis."[32] The American Bar Association argues that:

> [p]rivacy rights… have been eroded because, in the wake of 9/11, Congress dismantled the "wall" between government surveillance for domestic law enforcement purposes and surveillance activities for foreign-intelligence gathering.[33]

II. A SINGAPORE CASE-STUDY

Singapore has adopted the following measures against carriers and to protect the vulnerable.

Susceptible people are referred to as "at-risk individuals" under the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020, which was made on 25 March 2020 by the

---

[30] Quasi-quarantine measures allow an individual subjected to it limited access to others (whereas quarantine measures, on the other hand, ensure that individuals subjected to it are not supposed to come into contact with others at all in order to avoid the possibility of the spread of the virus through person-to-person contact) (see "Everything you need to know about Quarantine Orders", *Government of Singapore* (25 March 2020) <http://www.gov.sg/article/everything-you-need-to-know-about-quarantine-orders> (accessed 31 March 2020))

[31] Hariz Baharudin, "Coronavirus: S'pore contact tracing app now open-sourced, 1 in 5 here have downloaded", *The Straits Times* (10 April 2020) <http://www.straitstimes.com/singapore/coronavirus-spore-contact-tracing-app-now-open-sourced-1-in-5-here-have-downloaded> (accessed 12 April 2020)

[32] Henry De Valence, "Let's Develop Decentralized, Privacy-Preserving Contact Tracing", *Zcash Foundation* (23 March 2020) <http://www.zfnd.org/blog/decentralized-contact-tracing/> (accessed 30 March 2020)

[33]Hina Shamsi & Alex Abdo, "Privacy and Surveillance Post-9/11", *American Bar Association* (1 January 2011) <http://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/> (accessed 31 March 2020)

Minister of Health under powers conferred to him by virtue of s73 of the Infectious Diseases Act[34] (hereinafter referred to as "the IDA"). This includes an individual who:

> enters Singapore (by land, sea or air) from a country or territory outside Singapore during the control period;
> before or during the control period, comes into contact or has come into contact with any other individual who is, or is suspected to be, infected with COVID-19;
> has, before or during the control period, undergone a test to determine whether he or she is infected with COVID-19 and the test result is pending or uncertain; or
> at any time during the control period appears to the specified person to be or have been exposed to the risk of becoming infected with or a carrier of COVID-19.[35]

The primary mean which Singapore employs to isolate susceptible people is via the issuance of a Stay-Home Notice ("SHN"). In addition to SHNs, the Singapore Government has also been encouraging its citizens to download and use an app known as TraceTogether, which will assist the relevant authorities to carry out contact tracing should it be required. Each will be discussed in turn.

1. Stay-Home Notice

Prior to the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020, a 14-day SHN was issued to all travellers entering Singapore (inclusive of all Singaporeans, Permanent Residents, Long Term Pass holders and short-term visitors) and exhibiting fever and/or other symptoms of respiratory illness with a negative COVID-19 swab test from 13 March 2020. All travellers who refused to undergo the COVID-19 swab test when requested could be prosecuted and face penalties. From 20 March 2020, 2359h, tighter measures, in the form of a 14-day SHN were issued to all travellers entering Singapore.[36]

The power to issue an SHN (prior to the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020) is found under s15(2) IDA, which confers powers on the Director of Medical Services to "order any person who is, or is suspected or continues to be suspected to be, a case or carrier or contact of an infectious disease, or who has recently recovered from or been treated for such disease, to remain and to be isolated and (if necessary) be treated, in his own dwelling place —

> for such period of time as may be necessary for the protection of the public; and
> subject to such conditions as the Director may consider necessary for this purpose."

Persons under a 14-day SHN must remain in their place of residence at all times, during the 14-day period. They may not leave their residence, even if it is to purchase food and

[34] Cap 137, 2003 Rev Ed
[35] Reg 2 of the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020
[36] "Updates on COVID-19 (Coronavirus Disease 2019) Local Situation), *Ministry of Health, Singapore* <http://www.moh.gov.sg/covid-19> (accessed 31 March 2020)

essentials or to attend to important personal matters, save for circumstances whereby medical attention is required.[37][38]

Any person who is subjected to a 14-day SHN and leaves the place of accommodation specified in the SHN during the period specified in the SHN without reasonable excuse is guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 and to imprisonment for a term not exceeding 6 months or to both.[39]

If a Singapore Permanent Resident, Long-Term Visit Pass holder, Dependant's Pass holder, or Student's Pass holder fails to comply with a 14-day SHN, his/her respective Re-Entry Permit or passes may be revoked, or the validity shortened. If a foreign employee issued with a work pass fails to comply with a 14-day SHN, his/her work pass may be revoked pursuant to s7 (4)(a) of the Employment of Foreign Manpower Act. If a full-time student attending a preschool, school or other educational institution in Singapore fails to comply with a 14-day SHN, the student may be subjected to disciplinary action, including suspension or dismissal. For foreign students, this may include the cancellation of your child's/ward's Student's Pass or Dependant's Pass.[40]

a. Ensuring compliance with a 14-day Stay-Home Notice: Legislative framework

The IDA confers powers on the Director of Medical Services to take necessary steps to ensure that a susceptible person issued with a 14-day SHN comply with it. s15(2)(b) provides that a susceptible person is to remain and to be isolated "subject to such conditions as the Director may consider necessary for [the protection of the public]." s15(2)(b) therefore allows the relevant authorities to impose conditions/measures upon such isolation which a susceptible person would have to comply with during a 14-day SHN. Such measures include reporting on their present whereabouts, which will be discussed further below.

Further, Reg 7A 1)(d) of the Infectious Diseases (Measures to Prevent Spread of COVID-19) Regulations 2020[41] (made on 26 March 2020) provides that "an individual who is subject to a movement control measure requiring the individual to not leave a place of accommodation commits an offence if the individual, without reasonable excuse is not contactable by the Director or a Health Officer, or any individual acting on behalf of the Director or a Health Officer, at any reasonable time." Reg 7A (3) provides that an

[37] "Everything you need to know about Stay-Home Notice", *Government of Singapore* (19 March 2020) <http://www.gov.sg/article/everything-you-need-to-know-about-the-stay-home-notice> (accessed 30 March 2020)
[38] See also Reg 4(3) of the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020 as amended by the Infectious Diseases (COVID-19 – Stay Orders) (Amendment) Regulations 2020
[39] See s21A IDA and Reg 4(1) and (2) of the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020 as amended by the Infectious Diseases (COVID-19 – Stay Orders) (Amendment) Regulations 2020
[40] "Everything you need to know about Stay-Home Notice", *Government of Singapore* (19 March 2020) <http://www.gov.sg/article/everything-you-need-to-know-about-the-stay-home-notice> (accessed 30 March 2020)
[41] As amended by the Infectious Diseases (Measures to Prevent Spread of COVID-19) (Amendment) Regulations 2020

individual who fails to comply with Reg 7A (1)(d) "shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 6 months or to both." Therefore, it is a criminal offence if a susceptible person under a 14-day SHN is not contactable within reasonable time and that such contact can be made for the purposes of ascertaining the whereabouts of a susceptible person.

From the perspective of criminal sanctions, a recipient of a 14-day stay at home notice (SHN) may be subjected to two types of criminal offences:

> Firstly, failure to comply with a 14-day SHN by leaving the place of accommodation specified in the SHN during the period specified in the SHN is a criminal offence under s21A IDA and/or Reg 4 Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020.
> Secondly, failure to be contactable while subjected to a 14-day SHN is a criminal offence under Reg 7A Infectious Diseases (Measures to Prevent Spread of COVID-19) Regulations 2020 (read with Reg 7(4)).

There have been no additional powers conferred to the relevant enforcement authorities via legislation or subsidiary legislation in terms of investigation, search, seizure, detention, etc, since 31 December 2019. Prior to the COVID-19 pandemic, the IDA already provides powers for the relevant authorities to carry out any necessary investigation and enforcement for any offences committed under the IDA.

A "Health Officer" as constituted under s4 IDA may qualify as a form of "civil policing", i.e. non-police investigation and enforcement. s4(1) IDA provides that the Director of Medical Services, the Director-General of the Public Health or the Director-General of Food Administration may appoint any public officer or officer of any statutory body or employee of a prescribed institution to be a "Health Officer" for the purposes of the IDA. Further, s4 (2) IDA provides that the Director of Medical Services, the Director-General of the Public Health or the Director-General of Food Administration may delegate to any "Health Officer" all or any of the powers conferred on him under the IDA.

> ss55A (1)(a)(i) and (b) IDA provides that for the purposes of an investigation into an offence punishable under the IDA, any police officer, or any Health Officer, may require any person to furnish any information within his knowledge or at any time without warrant and with such force as may be necessary, stop, board, enter, inspect and search any premises or conveyance.
>
> s56(1) IDA provides that any police officer, or any Health Officer, may arrest without warrant any person committed or who he has reason to believe has committed any offence under, *inter alia*, s21A(4) IDA (which refers to the criminal offence committed if one leaves his/her place of accommodation before the 14-day SHN expires).
>
> s56(3)(a) IDA also provides that any police officer, or Health Officer, may arrest without warrant any person who being required to be isolated in any place under the provisions of the IDA, has failed to proceed to that place or has left or attempted to leave that place. As an alternative to arrest, s56(7)(a) IDA provides

> that a police officer or Health Officer may take such measures as he thinks fit in a case where that person is to be isolated: (i) to cause that person to be taken to the place where he is to be isolated; or (ii) to ensure that the person remains in isolation in his own dwelling place, for such period of time and subject to such conditions as necessary for the protection of the public. s56(8) IDA further provides that the measures referred to in s56(7) may extend to the entry into any premises without a warrant and the use of such force as may be necessary.

Therefore, broad powers are conferred on Health Officers to investigate, enforce and ensure compliance with a 14-day SHN and it should be noted that s4, ss55A(1)(a)(i) and (b), ss56(1), 3(a), (7)(a) and (8) IDA were already in force no later than 1 April 2019, which is well before the COVID-19 pandemic.

b. Surveillance capacities

It should be noted that even though s16(1) IDA confers powers on the Director of Medical Services to "order any person who is, or is suspected to be, a case or carrier or contact of an infectious disease to undergo surveillance for such period of time and subject to such conditions as the Director thinks fit", this does not permit the relevant authorities to carry out surveillance on susceptible persons in the more limited definition of the word. Merriam-Webster defines "surveillance" as "close watch kept over someone or something (as by a detective)". This is different from the definition of "surveillance" provided under s2 IDA, which provides that "surveillance" means "subjecting a person or persons to medical examinations or observations carried out over a period of time (whether or not continuously) and includes carrying out any measures to facilitate those medical examinations or observations".

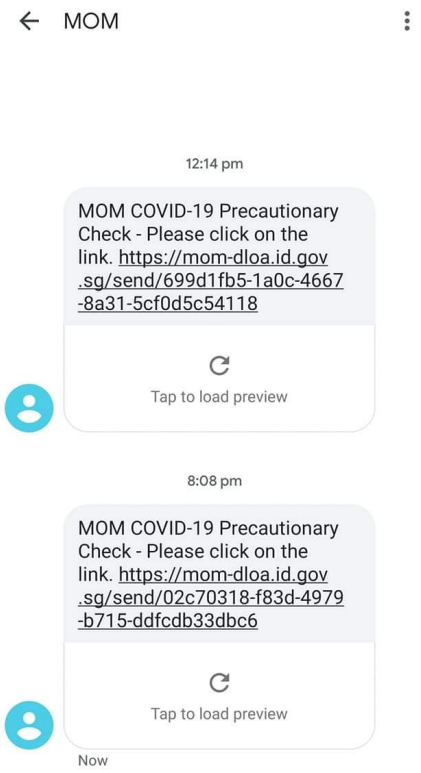
To ensure compliance with a 14-day SHN, the Immigration and Checkpoints Authority ("ICA") have required individuals to prove their whereabouts via the following methods[42]:

> Text messages are sent at various times in a day to persons issued with the SHN. They are then required to update ICA of their location within an hour, through their phone's GPS location service via a unique web link provided in the text message. This will be referred to as Method 1.
>
> ICA officers will also make random phone calls and house visits, including to those who do not respond to the text messages or phone calls. Those who get the phone call must take photos of their surroundings to verify their whereabouts. This will be referred to as Method 2.

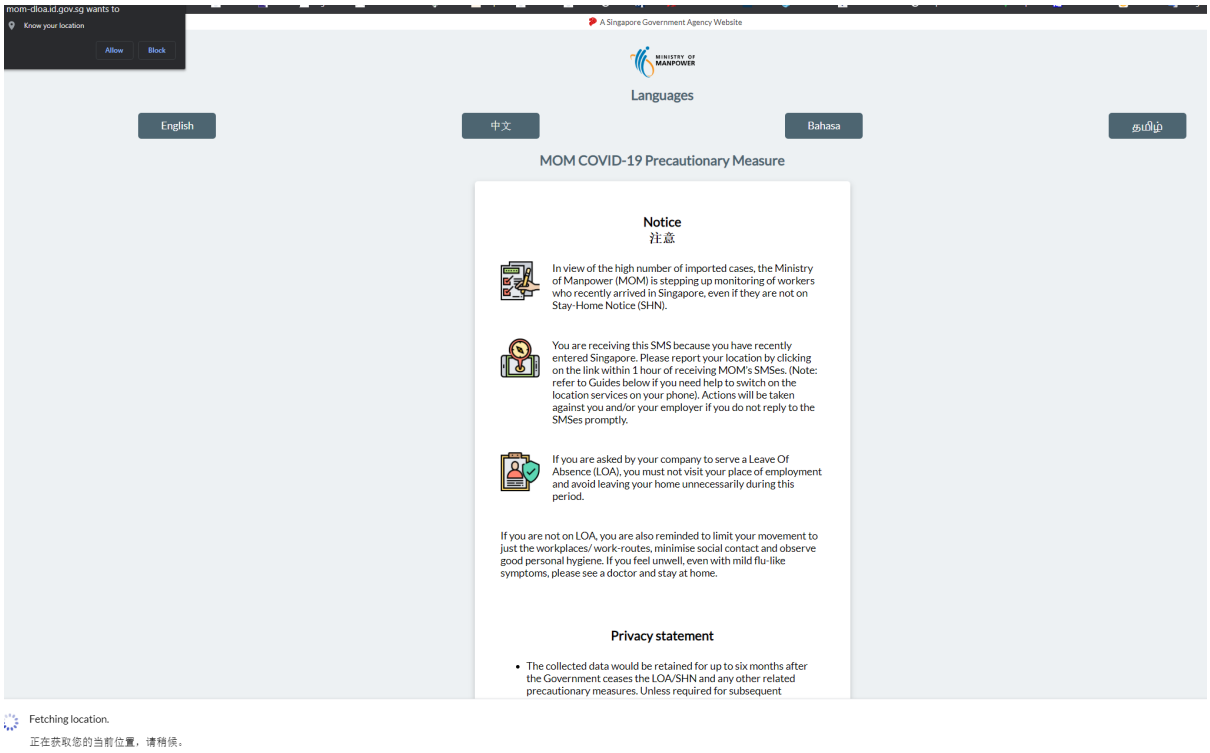
Method 1 works in the following manner:

[42] Aqil Haziq Mahmud, "More than 7,000 Stay-Home Notices issued for COVID-19; checks done through GPS, photos: ICA", *Channel News Asia* (12 March 2020) <http://www.channelnewsasia.com/news/singapore/covid-19-coronavirus-ica-7000-stay-home-notice-enforcement-gps-12530060> (accessed 30 March 2020)

Text messages are sent by the Ministry of Manpower ("MOM") at various times in a day to persons issued with the 14-day SHN, which look like this:



Clicking on the link opens the web browser, which then brings the recipient to this webpage:



The "Notice" on the Ministry of Manpower's ("MOM's") webpage prompts and guides the recipient to turn on location services on his/her mobile phone. The web browser notifies the recipient that "[The webpage] wants to: Know your location". The recipient then accepts the request and the web browser sends the location of the mobile phone (determined by GPS) to MOM's webpage.

The "Privacy Statement"[43] on the webpage provides as such: "The collected data would be retained for up to six months after the Government ceases the LOA/SHN and any other related precautionary measures. Unless required for subsequent enforcement follow-up, the collected data would be destroyed once the retention period lapses. The collected data would not be used or shared for purposes other than for ensuring your compliance with the LOA/SHN or precautionary measures."

Method 1 is otherwise known as a HTML5 geolocation Application Programming Interface ("API") and retrieves the recipient's location in 2 ways[44]:

> *Getting the current position method*: This method initiates an asynchronous request to detect the recipient's current position via the mobile phone's GPS hardware.
> *Watching the current position method*: This method works via a call back function which allows the web browser to update the recipient's location as the recipient moves.

[43] Despite the absence of a constitutional right of privacy in Singapore, the reference here recognises at least on a reflective level that chalenges to the integrity of individual data poses a sufficient risk to privacy requiring a privacy declaration. A less generous interpretation is that the statement represents little more than a conventional compliance provision.

[44] "Using the Geolocation API", MDN web docs (2 April 2020) <http://developer.mozilla.org/en-US/docs/Web/API/Geolocation_API/Using_the_Geolocation_API> (accessed 30 April 2020)

On a balance of probabilities, however, it is unlikely that that the *watching current position method* would be the preferred. Firstly, to stop the web browser from updating the recipient's location to the webpage, all that needs to be done is to close the connection between the webpage and the web browser. For example, by closing the webpage in the web browser. Secondly, if "watching the current position" was the method chosen, it would be unnecessary to send multiple texts to recipients in a day at random times for them to carry out the same process again.

Using the HTML 5 geolocation API, the MOM webpage does not (and would not be able to) retrieve any other form of data from the recipient's mobile phone e.g., history of credit card transactions made on the mobile phone or history of places where the recipient may have been. Method 1 is therefore inherently limited by the technology employed for its purpose.

Method 2 simply provides for house visits to be made and/or requires the recipient of the phone call from ICA to take photos of their surroundings in order to verify their whereabouts at random timings. This is all carried out by manual labour.

If, the relevant authorities are carrying out surveillance on recipients of a 14-day SHN, it is unlikely that would be an issue of whether valid "consent" was given for such surveillance via compliance with Methods 1 and 2. The recipients of a 14-day SHN simply do not have a choice but to comply with Methods 1 or 2 if and when used on them because non-compliance is likely to lead to the recipient having committed a criminal offence pursuant to Reg 7 of the Infectious Diseases (Measures to Prevent Spread of COVID-19) Regulations 2020.

In other words, one cannot be said to have "consented" to (and henceforth authorised) surveillance by complying with Methods 1 or 2. It is difficult to see how valid "consent" can be given when one performs an action to comply with the law, i.e. it is either one "consents" or doesn't "consent" and subsequently gets fined or jailed. For example, if one were to file his tax returns on time (in order to avoid criminal sanctions), can one be said to have "consented" to the State knowing what his annual income is.

It is noteworthy to point out that there is no constitutional right to privacy in Singapore.[45] That said the legislature does recognise the importance of personal data protection in private sector usage. In addition, privacy protection statements are common in the use of major data platforms in Singapore.[46]

2. TraceTogether App

[45] *Lim Meng Suang v AG* [2015] 1 SLR 26

[46] There is not time here to do justice to a comparative analysis of the standing of privacy protections in individualist settings such as the EU and in more communitarian traditions in some Asian states. In order to avoid a tokenistic duality we do recognize that in certain contexts privacy as a right may be a second order concern depending on context and cultural/socia/institutional externalities. The paper also directs what might be privacy challenges into the more neutral realm of data integrity. CAIDG is exploring privacy relativities in more detail.

TraceTogether is a mobile application developed by GovTech Singapore in collaboration with Singapore's Ministry of Health, which assists in contact tracing, if and when required. Downloading and activating TraceTogether is entirely voluntary, i.e. it is not a criminal offence if one does not download and activate the TraceTogether app. The National Development Minister commented recently that a take-up rate of one million Singaporeans was not enough for it to be truly effective.[47]

TraceTogether works by advertising a Temporary ID over Bluetooth Low Energy technology ("BLE"). When two devices (with TraceTogether installed and activated) are co-located within BLE range, they can detect each other and record this encounter in the local storage.[48] These records will then be stored locally in the users' phones.

If a user of TraceTogether tests positive for COVID-19, users will be asked to share these records when contacted by the Ministry of Health as part of contact tracing investigations. This therefore facilitates (instead of relying on one's memory) and greatly speeds up the contact tracing process, which is crucial to limit the spread of the Virus. TraceTogether acts as a pre-emptive tracing method as it tracks the people a non-susceptible person comes into contact with in his/her daily activities.

TraceTogether does not access a user's phone contact list or address book, nor does it collect or use location data automatically. Obviously, the purpose of the app is as a locator, but that information is provided by the user. TraceTogether seeks to establish who may have been exposed to the virus and not where such exposure may have taken place.[49] To ensure transparency of the app, the APK file of TraceTogether is made publicly available.[50]

TraceTogether serves as a form of decentralised contact-logging and contact tracing. [51]

3. Whether the data procured through MOM monitoring complies with personal data protection guidelines in Singapore

It should firstly be noted that the Personal Data Protection Act ("PDPA") generally does not apply to "any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data".[52]

Clara Chong "About 1 Million People Have Downloaded Trace Together App But More Need to do o or it to be Effective: Lawrence Wong". *Straits Times* (1 April 2020) <https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for> (accessed 4 May 2020)

[48] Meshead, "TraceTogether: A Technical Look", *Medium* (24 March 2020) <http://medium.com/@meshead/tracetogether-a-technical-look-e48360d4a4a9> (accessed 30 March 2020)

[49] Tang See Kit & Aqil Haziq Mahmud, "Singapore launches TraceTogether mobile app to boost COVID-19 contact tracing efforts", *Channel News Asia* (20 March 2020) <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616> (accessed 31 March 2020)

[50] "TraceTogether 1.7.0 APK for Android", *APK4FUN* (30 April 2020) <http://www.apk4fun.com/apps/sg.gov.tech.bluetrace/> (1 May 2020)

[51] Henry De Valence, "Let's Develop Decentralized, Privacy-Preserving Contact Tracing", *Zcash Foundation* (23 March 2020) <http://www.zfnd.org/blog/decentralized-contact-tracing/> (accessed 30 March 2020)

[52] s4(1)(c) PDPA.

Consequently, the various obligations under the PDPA relating to consent, purpose limitation, notification, access and correction, accuracy, protection, retention limitation, transfer limitation, etc, do not apply to public agencies.

Data collected by the public sector is instead protected by specific legislation such as the Official Secrets Act, the Income Tax Act, the IDA, etc. Additionally, the Government Instruction Manuals (which are not publicly available) include measures to govern the use, retention, sharing and security of personal data among public agencies.

The Public Sector (Governance) Act 2018 ("PSGA") was also introduced in 2018 to provide for additional safeguards for personal data in the public sector, including criminalising the misuse of data by public servants. For example, s7(1) PSGA provides that if an individual discloses, or the individual's conduct causes disclosure of information, under the control of a Singapore public sector agency to another person (whether or not a Singapore public sector agency); the disclosure is not authorised by any data sharing direction given to the Singapore public sector agency; the individual is a relevant public official of the Singapore public sector agency at the time of the disclosure; and the individual does so knowing that the disclosure is not in accordance with that direction; or reckless as to whether the disclosure is or is not in accordance with that direction, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.

Specifically, the IDA governs when relevant information may be collected and disclosed. For example, ss 57A and B provides for circumstances where the Director of Medical Services would be able to disclose information to prevent spread or possible outbreak of infectious disease.

Following on from the Singapore tracing/tracking and surveillance observations it is useful to briefly contrast the surveillance activity in the PRC, a state with a recent history of employing technology in an array of citizen oversight contexts, that may represent challenges to civil rights and individual dignity if such technologies and the data they source outlive the crisis exigencies (as discussed in more detail in the paper's final sections).

III. THE PEOPLE'S REPUBLIC OF CHINA ("THE PRC") CASE STUDY

1. Legislative backdrop

Broad powers are conferred on the relevant authorities in the PRC to handle the COVID-19 pandemic. Save for the National Health Commission of the PRC stating that the Virus would be regulated as a Class A infectious disease (albeit classified as a Class B infectious disease) under the Law of the PRC on the Prevention and Treatment of Infectious Diseases ("中华人民共和国传染防治法")[53] (hereinafter referred to as "the PTID") on

[53] "中华人民共和国传染病防治法", *The Central People's Government of the People's Republic of China* (1 August 2005) <http://www.gov.cn/banshi/2005-08/01/content_19023.htm> (accessed 2 April 2020)

20 January 2020[54] (i.e. to ensure that COVID-19 falls under the legal ambit of the PTID), there does not seem to be any other new legislative and/or administrative authorisations enacted in the PRC in relation to COVID-19.

As will be demonstrated below, the existing express provisions in the relevant legislation in the PRC related to the handling of the COVID-19 pandemic are generally wide enough to legally empower both state and local authorities to take the necessary centralised and decentralised types of actions as seen thus far. In other words, there will be considerable difficulty in arguing that both the state and local authorities had acted *ultra vires* in carrying out the examples of quasi-quarantine measures and pre-emptive contact tracing methods which will be discussed below.

a. Power to implement pre-emptive tracing methods and to utilise both state and non-state resources/machinery to do so

Power to carry out pre-emptive contact tracing

Art 12 PTID provides that all organisations and individuals within the territory of the PRC must subject themselves to the investigations, examinations, sample gathering, isolation, treatment and *other relevant epidemic prevention and control measures* taken by the epidemic prevention and control organisations and medical organisations and to provide such information as required truthfully. [emphasis added]
Art 12 PTID provides safeguards whereby the said epidemic prevention and control organisations and medical organisations are not to disclose relevant information and data which are personal and private. Affected organisations and individuals can seek redress via administrative reviews or litigation.

The Emergency Response Law of the PRC ("中华人民共和国突发事件应对法")[55] (hereinafter referred to as "the ERL") similarly governs the COVID-19 pandemic. Art 3 ERL defines an emergency incident as one including a public health incident which have caused or may cause serious harm to the society and therefore requires the adoption of emergency response measures.

Art 49 ERL provides that after the occurrence of a public health incident, the People's Government (i.e. the local state authorities) performing the responsibility for uniform leadership may adopt any or more of the following measures for emergency response operations, which includes the taking of necessary measures to prevent the occurrences of secondary and derivative incidents (see Art 49(10)).

The broad powers conferred under Art 12 PTID and Art 49(10) ERL allows both the State and local authorities to take relevant measures it may deem appropriate during the

[54] "中华人民共和国国家卫生健康委员会公告 2020 年第一号", *The Central People's Government of the People's Republic of China* (21 January 2020) <http://www.gov.cn/xinwen/2020-01/21/content_5471158.htm> (accessed 2 April 2020)
[55] "中华人民共和国突发事件应对法（主席令第六十九号）", *The Central People's Government of the People's Republic of China* (30 August 2007) <http://www.gov.cn/flfg/2007-08/30/content_732593.htm> (accessed 2 April 2020)

COVID-19 pandemic and these provisions are broad enough to encompass pre-emptive measures such as pre-emptive contact tracing methods.

Power to utilise both state and non-state machinery to carry out pre-emptive tracing

Art 45 of the PTID provides, *inter alia*, that during the outbreak of an infectious disease, the National State Council has the power to mobilise manpower or to requisition reserve materials, housing, transportation tools and *other relevant facilities and equipment as required to control the outbreak* [emphasis added].

Art 49(5) of the ERL provides that one of the measures which may be adopted after the occurrence of a public health incident is the activation of the use of the People's Government fiscal reserve funds and emergency response rescue material in reserve, *and when necessary, mustering other materials, equipment, facilities and instruments for use* [emphasis added].

Art 52 ERL further provides, *inter alia*, that where necessary, the People's Government performing the responsibility for uniform leadership or organising the emergency response operations *may requisition equipment, facilities, premises, etc, from organisations and individuals*, request other local People's Governments to provide human, material and financial resources or technical support, etc [emphasis added].

The overarching broad power conferred to the relevant authorities under the PTID and the ERL allows for the carrying out of pre-emptive contact tracing methods utilising both state and non-state resources and machinery in order to do so.

Power to impose quasi-quarantine measures and to ensure adherence thereof

Art 39 PTID provides, *inter alia*, that upon discovery of a Class A infectious disease, the following persons are to be classified and handled as such:

> Infected persons are to be isolated and treated for a duration to be medically determined
> People who are suspected to be infected are to be isolated and treated prior to confirmation of infection at a designated venue

The PRC's definition of susceptible people: Persons in close contact with infected persons, people who were originally infected and persons suspected to be infected are to be medically observed and *all other relevant preventive measures are to be taken at a designated venue* [emphasis added]

An official annotation of the PTID provided by the National People's Congress of the PRC states that Art 39, with regard to susceptible people, a "designated venue" can be both inside and outside a medical organisation so long as such persons are isolated. Such isolation periods ought to exceed the incubation period of the respective infectious disease.

Taking all other relevant preventive measures is defined to mean appropriate medical intervention, such as vaccination and the oral administration of medicine, etc.[56]
Art 39 is broad enough to empower the relevant authorities to take any required quasi-quarantine measures on susceptible people at their respective homes and to ensure that such persons adhere to such quasi-quarantine measures.

2. Some technology-driven applications for surveillance

a. One QR code for every stop/station, one QR code for every car/carriage ("一站一码，一车一码")

From 6 February 2020, under the guidance of the Shenyang Municipal Transportation Bureau, Meituan developed a platform which allows for the tracking of the movement of citizens using public transport in Shenyang. QR codes are affixed to subway stations, subway carriages, public buses, trams, taxis, etc, in order to achieve "one QR code for every stop/station, one QR code for every car/carriage".[57]

Passengers of such modes of public transport would have to scan these QR codes with their WeChat app during boarding and alighting. Scanning the QR code uploads the passenger's contact information onto the platform developed by Meituan. The data is uploaded onto a private server and encrypted. For those without mobile phones, manual registration would be done.

This serves as a pre-emptive tracing method as it allows for the daily tracking of a particular passenger's movement via public transport in order to facilitate contact tracing as and when required. This acts as a centralised contact-logging and a non-privacy preserving pre-emptive tracing method.

b. Smart doorbells ("爱心门铃")

On 11 March 2020, in order to limit imported cases of COVID-19, Beijing announced that all international arrivals into Beijing are to undergo a 14-day self-quarantine at home.[58] The 14-day self-quarantine imposed by the Beijing local government is similar to a 14-day SHN as a quasi-quarantine measure.

In order to ensure that individuals adhere to this 14-day self-quarantine, local communities in the Shijingshan and Haidian districts in Beijing are using smart doorbells

---

[56] "中华人民共和国传染病防治法释义，第三十九条", *The National People's Congress of the People's Republic of China* (5 August 2005) <http://www.npc.gov.cn/zgrdw/npc/flsyywd/xingzheng/2005-08/05/content_353234.htm> (accessed 2 April 2020)
[57] 冉晓宁，"美团打车助力沈阳实名登记乘车"一站一码，一车一码"疫情防控可追溯", *Xinhua News Agency* (8 February 2020) <http://www.xinhuanet.com/enterprise/2020-02/08/c_1125547006.htm> (accessed 2 April 2020)
[58] Wallis Wang, "Self-quarantine of all international travellers to Beijing as China fights import of coronavirus", *South China Morning Post* (12 March 2020) <http://www.scmp.com/video/china/3074787/self-quarantine-all-international-travellers-beijing-china-fights-import (accessed 2 April 2020)

"with a monitoring function to ensure strict enforcement of home isolation."[59] Installation of the smart doorbell is optional for those who return to Beijing from other parts of China but is compulsory for those who return from overseas.

The smart doorbell is also dubbed as an "爱心门铃" or care doorbell. Individuals under self-quarantine can press the doorbell to connect to the community worker's mobile phone and then have a video chat with them in order to request for assistance (e.g. to purchase groceries).[60]

The smart doorbell is developed by Xiaomi Technology and has a camera affixed to it.[61][62] Upon detection that there is a change in the environment or status of the door (e.g. where there is a visitor or where the door is opened), a Mijia app (Xiaomi Home app) installed on a community worker's phone will receive an alarm and a 6-second real-time monitoring video from the camera. This would therefore allow the community worker to monitor any changes that happens at a quarantined individual's door and is therefore a piece of technology adopted to ensure adherence to the quasi-quarantine measures.

This application is still somewhat limited in nature as the surveillance is limited to the area outside one's door and is only active as and when a change in the environment outside the door is detected.

The following section is offered in the form of the writer's direct observations and without additional critical commentary, as an example of the approach to reservations offered in Chinese contemporary scholarship.

Prof Hu Yong's commentary

At this point, to offer an internal view of developments in China the paper indulges in a brief review by a respected PRC academic. Prof Hu Yong from the Peking University School of Journalism and Communication recently wrote a commentary (in Chinese) dated 8 March 2020 titled "Public interest and personal privacy during a crisis".[63] The salient points follow.

Prof Hu notes that during major outbreaks of an infectious disease, timely access to relevant data is critical. Firstly, it is important to know who was in close contact with an infected person or who was in the same flight or train journey as them. Secondly, it is important to know who shares the same residence with an infected person and the neighbourhood which they are located in. Thirdly, it may also be important to gather the geolocation history and data in order to trace and find out the places where an infected

[59] "High-tech means applied in Beijing's isolation administration", *Global Times* (31 March 2020) <http://www.globaltimes.cn/content/1184336.shtml> (accessed 2 April 2020)
[60] 鲍聪颖&高星，"石景山：为居家观察者安装'爱心门铃'", *人民网* (22 March 2020) <http://bj.people.com.cn/BIG5/n2/2020/0322/c82838-33894667.html> (accessed 2 April 2020)
[61] 冉晓宁，"石景山 1500 万资金助力'科技抗疫'", *Xinhua News Agency* (11 April 2020) <http://www.xinhuanet.com/tech/2020-04/11/c_1125841046.htm> (accessed 1 May 2020)
[62] Dlingsmart website <http://www.dlingsmart.com/> (accessed 2 April 2020)
[63] 胡泳，"胡泳：危机时刻的公共利益与个人隐私"，*胡泳的博客* (11 March 2020) <http://huyong.blog.caixin.com/archives/223460> (accessed 2 April 2020)

person had been too. In practice, public health monitoring is a data-intensive exercise which inevitably raises issues regarding personal privacy.

Prof Hu then attempts to define what privacy entails. He notes that there are three views to privacy. Firstly, a right to non-interference. Secondly, a right to control the means and timing which one's personal information is to be disclosed. Lastly, a right to be left alone. If one were to adopt these three views of what privacy entails, public health monitoring during the novel coronavirus crisis brings about a startling infringement of one's privacy. Prof Hu espouses three principles in relation to striking a balance between the public interest and personal privacy. From the outset, he notes that this is not an easy task. This is especially so where a country faces crises in relation to safety and health where it is difficult to draw a line between information which should be regarded as personal (and therefore conferred protection upon) and information which must be accessible to all in the name of public interest (even if an affected individual would want to keep such information private).

He argues that the first and foremost principle in this regard is to treat the public interest as an exception to privacy. Professor Hu speculates that the general public in China recognises that there is great value in the reporting or disclosure of certain information in order to promote the welfare of society. This includes information relating to illegal activities and persons involved thereof, protection of public safety, national defence, curbing the outbreaks of infectious diseases, etc. In such cases, due consideration ought to be given to the relative seriousness under each particular context and if the circumstances require as such, one's right to personal privacy can be reduced for the public interest. But this must be an exception and not the rule.

The second principle is that if it is really necessary to restrict one's right to privacy for the sake of public interest, appropriate safeguards must be put in place to protect one's right as a private citizen and their respective personal interests in the process of protecting the public interest. We must be cognisant of the fact that even though at times we have to bear in mind the broader public interests at hand and therefore restrict one's rights to privacy, privacy itself is also an important public interest. Public interest is not confined to matters concerning the public only, such as governmental regulation or the administration of justice. Public interest also lies in the protection and enforcing of individual freedoms, rights and interests.

The third principle is that fair use of such information must be insisted upon. Due to the great amount of information which is personally sensitive that has been aggregated through multiple channels, major challenges are posed regarding how such information is to be safely stored and exploited.

IV. COMPARATIVE GLOBAL RESPONSES

This section builds on the two detailed case studies to classify the different types of control actions taken in other parts of the world, to clarify more thematically what commentators are critiquing when they talk about "contact tracing" or "using tech to

address COVID". Crucial in this process of understanding is to identify what type of information is needed through these surveillance and tracing technologies, for what purposes, and whether these are not being achieved or in fact are exceeded. For instance, using Bluetooth low energy for proximity tracking is currently popular in tracing and tracking. This approach may be adequate for the initial "identification" step of contact tracing but identified location data still might be needed to enforce quarantines or identify hotspots.

In general, public health authorities use Information and Communications Technologies ("ICT") for: diagnostic efforts (assessing how a disease is spreading and the nature of the risks), coordination processes (coordinating between different response actors), and risk communication (talking to the general public).[64]

In the current pandemic, much effort and attention are aimed at diagnostic efforts.

1. Clarifying contact tracing

To reiterate, the main goal of contact tracing is to identify close contacts of confirmed cases. As for its extant purpose, tracing follows individual movement and plots/records human contact so that potential transmission will be revealed. It is not difficult to imagine how such data on movement and association may also present a variety of other control and social engineering purposes. In this regard identification of data subjects is crucial, as are their patterns of movement and association. Even if the data subjects are given case names (such as in Singapore) linking back to actual identity is easy and intended. Closely related is the follow-up process: informing close contacts, asking these people to stay home, and/or sharing the locations that positive cases have visited. Contact tracing is part of the larger project of using ICTs to address disease outbreaks. Again, the identities of associates will be known and shared, as will be patterns of movement.

a. Tracing

The 'first generation' of manual contact tracing programs aim to identify close contacts *after* someone tests positive. These programs are usually targeted. Confirmed cases are often interviewed, and their verbal recount is supplemented by CCTV footage, card usage, and/or phone location data. Implementing these programs requires significant human intervention and rely on some pre-existing surveillance capabilities.[65]

---

[64] Christopher Wilson and Maria Gabrielsen Jumbert, 'The New Informatics of Pandemic Response: Humanitarian Technology, Efficiency, and the Subtle Retreat of National Agency', *Journal of International Humanitarian Action* 3, no. 1 (30 May 2018): 8, https://doi.org/10.1186/s41018-018-0036-5; Brooke Fisher Liu and Sora Kim, 'How Organizations Framed the 2009 H1N1 Pandemic via Social and Traditional Media: Implications for U.S. Health Communicators', *Public Relations Review* 37, no. 3 (1 September 2011): 233–44, https://doi.org/10.1016/j.pubrev.2011.03.005.

[65] Aqil Haziq Mahmud, "SAF making thousands of calls a day to contact trace, check stay-home compliance as COVID-19 fight hits 'critical juncture'", *Channel News Asia* (4 April 2020), <https://www.channelnewsasia.com/news/singapore/saf-contact-trace-stay-home-notice-shn-covid-19-12606752> (accessed 27 April 2020)

Automated tracing programs apply to the public at large, not just confirmed cases. Public health authorities encourage individuals to log of encounters which can quickly be referred to if a person tests positive. Follow-up actions (e.g. isolating close contacts) are facilitated, reducing the likelihood that carriers travel widely and spread the virus. One low-tech method to accomplish pre-emptive contact tracing is to make people scan QR codes to register every time they enter venues.[66] The ramifications of this data production and sharing in terms of rights of privacy, freedoms of movement and association, and containment of individual liberties are obvious.

Half the world's population carries a device well-suited to contact tracing, and this figure is 70-80% in developed countries. Phone-based tracking can further be decomposed into location and proximity tracing. Location tracing uses GPS and/or network information to identify the geographic location of the user. HaMagen (Israel) [67] and WeTrace (Philippines) [68] are examples of phone location tracking programs. Of course, the infrastructure to track people's location via smartphones already exists and is mostly in the hands of network service providers, phone manufactures, and technology companies. In certain arrangements, locator devices are only activated by the owner of the device.

Proximity tracking is less common (but not unheard of) in the current crisis armoury. Encounters are recorded, but the location of these encounters may be unknown. Proximity tracking is usually enabled by Bluetooth low energy. Many privacy advocates say that bluetooth proximity tracking is the least intrusive form of contact tracing, and it is emerging as the most popular approach more likely because of its utility and low cost. TraceTogether and the Pan-European Privacy-Preserving Proximity Tracing are prominent apps in this category.[69]

In the current pandemic, much effort and attention are aimed at diagnostic efforts. In particular, governments are using ICTs to (1) identify close contacts of confirmed cases and (2) maintain quarantines. In both these objectives participant identities are necessarily recorded, even if only to connect quarantine provisions with parties against whom they are directed. We now detail manual and automatic tracin in terms of purpose.

Manual contact tracing

Manual contact tracing programs aim to identify close contacts *after* someone tests positive. Confirmed cases are usually interviewed by human contact tracers, and their verbal recount is supplemented by CCTV footage, card records, and/or phone location

[66] Abacus, "Shanghai Introduces QR Codes on Subway to Track Potential Contact with Coronavirus", *South China Morning Post* (28 February 2020), <https://www.scmp.com/tech/article/3052880/shanghai-introduces-qr-codes-subway-track-potential-contact-coronavirus> (accessed 27 April 2020)
[67] "HaMagen - The Ministry of Health App for Fighting the Spread of Coronavirus", *Ministry of Health*, <https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/> (accessed 27 April 2020)
[68] "WeTrace – Community Tracing App – A Marriage between Technology and the Bayanihan Spirit!", *WeTrace*, < https://www.wetrace.ph/> (accessed 27 April 2020)
[69] https://www.tracetogether.gov.sg/; https://www.pepp-pt.org/
"TraceTogether", *GovTech* <https://www.tracetogether.gov.sg/> (accessed 27 April 2020); "Pepp-Pt. Pan-European Privacy-Preserving Proximity Tracing.", *Pepp-Pt* <https://www.pepp-pt.org> (accessed 8 April 2020)

data. Manual contract tracing requires manpower. Since late January, these programs have been implemented in countries that were relatively prepared like Singapore and South Korea. As we discuss later, manual approaches remain helpful even as automated programs gain prominence. The intention behind manual tracing is to produce a detailed personal history of infected subjects, covering more than movement and association, and including the nature, purpose, duration and coverage of movement and close human contact.

Automated contact tracing

As the pandemic has become more serious, governments (including relatively prepared ones) realised that faster, more scalable, and "pre-emptive" contract tracing methods are needed. Public health authorities want everybody to have a log of encounters which can quickly be referred to if a person tests positive. Follow-up actions (e.g. isolating close contacts) can happen faster, reducing the likelihood that carriers travel widely and spread the virus.

One relatively low-tech method to accomplish pre-emptive contact tracing is to make people scan QR codes to register every time they enter venues. This happened in several cities in China and in Singapore. But these methods have been replaced by more automated approaches.[70]

Phone-based tracking can further be decomposed into location and proximity tracing. Location tracing uses GPS and/or network information to identify the geographic location of the user. Automated tracing is intended as a more immediate, cost effective and widespread approach to tracing recording. Tracing for location may be in certain applications more dependent on the voluntary participation of parties.

In contrast, *proximity tracking records who a person has been in contact with, but not where.* Many privacy advocates say that pseudonymous Bluetooth proximity tracking is the least intrusive form of contact tracing, and it is emerging as the most popular approach to contact tracing.[71][72] Such programs are being developed or implemented in countries including Singapore (Trace Together), Europe (Pan-European privacy preserving proximity tracing), the UK, Norway, and the U.S.[73] On April 10, Google and Apple announced that they are partnering to make it easier for countries to develop Bluetooth contact tracing apps.[74]

---

[70] Abacus, "Shanghai Introduces QR Codes on Subway to Track Potential Contact with Coronavirus", *South China Morning Post* (28 February 2020) <https://www.scmp.com/tech/article/3052880/shanghai-introduces-qr-codes-subway-track-potential-contact-coronavirus> (accessed 27 April 2020)

[71] Hannah Murphy, "US and Europe Race to Develop "Contact Tracing" Apps'", *Financial Times* (3 April 2020), <https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95> (accessed 27 April 2020)

[72] "Pepp-Pt. Pan-European Privacy-Preserving Proximity Tracing.", Pepp-Pt <https://www.pepp-pt.org> (accessed 8 April 2020)

[73] Dave Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero* (9 April 2020) <https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9> (accessed 27 April 2020)

[74] "Apple and Google Partner on COVID-19 Contact Tracing Technology", *Apple Newsroom* (10 April 2020) <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/> (accessed 27 April 2020)

Since April, in the rush of excitement about Bluetooth proximity tracing, experts are beginning to warn that "automated contact tracing is not a panacea".[75] An automated contact tracing system is likely better than no system at all, but, where possible, such a system should augment rather than replace human contact tracers. First, human contact tracers are needed to make judgement calls about environment factors like ventilation. Second, following up with suspected close contacts involves "difficult and anxiety-laden conversations, and it is the role of a contact tracer to explain how a close contact might have been exposed...and provide assurance and guidance on next steps".[76]

2. Maintaining quarantines

Governments initially sought to quarantine and monitor specific people, for example close contacts of confirmed cases. As the pandemic has become more serious, governments have imposed widespread "lockdown" measures, thus the quarantine maintenance programs which accompany these measures have become more widespread too. While proximity tracing may be sufficient for identifying close contacts, location information is needed for quarantine maintenance. Programs for monitoring individuals under quarantine have been implemented in Argentina, Australia, China, Dubai, Ecuador, Hong Kong, India, Indonesia, Poland, Russia, Singapore, South Korea, Taiwan and Thailand.[77]

In Singapore, the 'second wave' of infections has largely occurred within migrant worker dormitories, where living conditions would make individual quarantining or spatial distancing unavailable. This situation has introduced much more stringent, and some might say demographically specific, quarantining that has produced a variety of other social and health threats for the quarantined population. The quarantine regime has been variegated to remove and protect presently healthy workers, while screening and treating many of those with the illness in the confines for the quarantine. There has also been attempts to depopulate the more crowded dormitories where habitation was less cramped when workers were outside the premises on shift-work rotation.

Quarantining and tracing have some interconnections insofar as they are both concerned with mapping and controlling patterns of movement. Additionally, governments seek to monitor general patterns of movement in populations, for example to identify potential clusters. Programs to monitor general movement are ongoing in Austria, Belgium, Brazil, Germany, Iran, Italy, Kenya, South Africa, and Switzerland.[78] We note that it is hard to

[75] Jason Bay, "Automated Contact Tracing Is Not a Coronavirus Panacea", *Medium* (14 April 2020) <https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98> (accessed 27 April 2020)
[76] Jason Bay, "Automated Contact Tracing Is Not a Coronavirus Panacea", *Medium* (14 April 2020) <https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98> (accessed 27 April 2020)
[77] Dave Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero* (9 April 2020), <https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9> (accessed 27 April 2020)
[78] Dave Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero* (9 April 2020), <https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9> (accessed 27 April 2020)

verify at what level of abstraction a given government is analysing location data, and governments are likely combining different approaches with problematic consequences for data integrity.

a. Quarantine containment

After the identification stage, public health authorities tend to inform close contacts and isolate them. They may use location-based methods to enforce said isolation.[79] Further, public health authorities may share information about these cases with the wider public, for example to warn the public about "hotspots". As a consequence of mass data sharing, governments must satisfy the public need for information about the crisis and its spread, without revealing information that will unnecessarily harm individuals or businesses.[80] Critical conversation Much critical conversation has revolved around contact tracing programs which collect names and location information, and how this information is shared in the follow-up stage.[81]

Proximity tracing with Bluetooth LE avoids many of the risks associated with non-anonymised contact tracing data, and hence its popularity.[82] However, the recent surge in proximity apps, and many still in development, means the critical discussion remains nascent. The data integrity challenges relating to Bluetooth proximity tracing apps will become clearer as various projects are rolled out in the coming weeks and months. These are some speculative challenges:

- Bluetooth mainly addresses issues related to identification rather than follow-up. Can they address how to monitor people who have been told to stay home?
- Location can be inferred from proximity to known locations. As a result, the remit of proximity-based apps could be expanded. In the UK, the NHS has internally discussed whether the app can be retooled to enforce social distancing, for example by warning people if they spend too much time outside.[83]
- Garnering high enough levels of adoption—50–75% of the population seems necessary. As of 4 April, about 16% of people in Singapore have downloaded TraceTogether.
- Coordination between different projects, especially in the U.S. Apps could crowd each other out and divide up the tracked population into even smaller chunks.
- Problematic security of Bluetooth technology.

---

[79] Dave Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero* (9 April 2020), <https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9> (accessed 27 April 2020)

[80] For example, if governments broadcast the travel history of confirmed cases without appropriate information about the exposure time frame, the public may inaccurately conclude that certain entire location are high risk, negatively affecting businesses in that location.

[81] See section 4 of "Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic".

[82] It is suggested that proximity tracing is more privacy protecting—this approach does not record the location of encounters. In some apps such as TraceTogether the assertion is that because data is collected on the phone and not the server this further protects privacy. For a caution on this see Harkness (2020).

[83] Gian Volpicelli, "The NHS coronavirus app could track how long you spend outside", *WIRED* (7 April 2020), <https://www.wired.co.uk/article/nhs-coronavirus-tracking-app> (accessed 27 April 2020)

One key question about the application of technology to the control of human movement relates to the essential nature of information needed and or what purposes. Proximity may be good enough for the *identification* step of contact tracing, but location data will be necessary to enforce quarantines or identify clusters. McDonald (2016) suggests that movement data or location data was not useful in tackling and predicting the spread of Ebola and MERS, partly because organizations did not have the capabilities to draw meaningful insights from large amounts of unprocessed data and poor coordination between organizations.

To add more detail to what has been in this section a random summarised coverage of world trends against themes behind the technology (such as identification, movement mapping, quarantine and the consequences for wider citizen safety) an appendix is provided at the conclusion of the paper to identify state preferences in technological capacity and data use.

The final substantive section indicates some significant challenges for ethical surveillance and mass data sharing within and beyond the period of the COVID-19 crisis. Of necessity this is a selective and speculative enterprise, requiring some guesswork on what might remain of the framework so described and the potentials this could offer to confound and compromise civil rights and human dignity measures. The section address challenges related to data rights, data integrity and intrusion into personal freedoms with surveillance ongoing.

V. ETHICAL CHALLENGES

This section moves from description and analysis in terms of expressed control objectives for a variety of technologies and data usages, to a more predictive discussion of consequences for mass data use beyond any determined limits of crisis containment. At the time of writing there are already many governments talking in terms of a phased return to employment, opening up of public transport, schools, and commercial activities that depend on association.[84] These strategies are risk/benefit in nature and involve contestation between economic and health interests. It is important to mention these developments so that any image of a clear and stable demarcation between crisis and post-crisis lifestyles is disabused. In presenting and discussing what we refer to as 'challenges' below, it is accepted that in any incremental or interconnected move away from crisis justifications, some of the objectives discussed above, and their justifications will not vanish. Looked at from a converse perspective, if control authorities who have the power to determine the nature, coverage and particularity of crisis control measures see these as diminishing or running in parallel with more conventional social intercourse, then the conversation about challenges that crisis objectives in situations of over-spill, is both important and even more complex. The brief reflection on 'crisis' mass data usage in non-health contexts presents a similar understanding of prevailing crisis objectives and diminished crisis purposes where new reasons for data use fail the crisis test and pose challenges to individual liberties.

[84] Marco Albani, "*There is no returning to normal after COVID-19. But there is a path forward*", *World Economic Forum*(15 April 2020) <https://www.weforum.org/agenda/2020/04/covid-19-three-horizons-framework/> (accessed 27 April 2020)

While during this crisis the world initially opened up to the sharing of personal data on a scale uncommon in times of conventional data use, spurred on by the desire either to be good citizens,[85] or to play a part in containing the virus, counter-narratives have emerged which rehearse reservations about the consequences of such mass data sharing. Urs Gasser from Harvard Law School's Berkman Klein Centre casts doubt on the risks and benefits in mining data to combat COVID-19, and aggregated mobility data in particular.[86] Gasser not only identifies privacy concerns but more pragmatic fit-for-purpose considerations. The Oxford Covid Impact Monitor[87] uses population movement data, provided by Cuebiq, which is a location intelligence and measurement platform. Through its Data for Good programme, Cuebiq offers access to aggregated and privacy-enhanced mobility data for academic research and humanitarian initiatives. They claim, "this first-party data is collected via anonymised users who have opted-in to provide access to their location data anonymously". Cuebiq basically shares their advertising tracking database governed by a privacy policy that pre-existed the COVID crisis and they have already been collaborating with partners in several "humanitarian" initiatives.[88] Oxford's website states: "Ethical big data can help save lives". However, there seems to be nothing on their website addressing ethical challenges beyond saying that they use anonymous data, which of itself does not address fairness issues or future misuses of data.

In a recent article entitled 'Can Your Smartphone Crack Covid?'[89] Timandra Harkness, from BBC Radio 4's *Future Proofing and How to Disagree* specifically engages the civil rights issues posed by a variety of Bluetooth tracing and tracking technologies the paper has identified above:

> I write constantly about the threat to privacy of letting our smartphones share data that reveals where we go, what we do, and who shares our personal space. And although these are exceptional circumstances, we should not stop valuing our privacy. Emergency measures have a habit of becoming the new normal. And information about who we've been close to could be of interest to all sorts of people, from blackmailers to over-enthusiastic police officers enforcing their own interpretation of "necessary activities".

In the context of these emergency measures and even their most legitimate objectives:

> The Chinese app, AliPay HealthCode, raises some red flags. It assigns users a unique QR code which displays red, yellow or green, indicating your health status, and which determines how much freedom of movement you're permitted. How that risk category is calculated remains opaque, though it uses proximity to known

[85] Cass R. Sunstein, *The Meaning of Masks*, FORTHCOMING JOURNAL OF BEHAVIORAL ECONOMICS FOR POLICY (2020). Available at: https://ssrn.com/abstract=3571428

[86] Urs Gasser, "How Much Access to Data be Permitted During the Covid-19 Pandemic?", *Harvard Law Today* (14 April 2020) <https://today.law.harvard.edu/how-much-access-to-data-should-be-permitted-during-covid-19-pandemic/?utm_source=hltTwitter> (accessed 27 April 2020)

[87] Oxford COVID-19 Impact Monitor, Oxford University <https://www.oxford-covid-19.com/> (accessed 27 April 2020)

[88] For some examples see Cuebiq Data For Good, *Cuebiq* <https://www.cuebiq.com/about/data-for-good/> (accessed 27 April 2020)

[89] Timandra Harkness, "Can Your Smartphone Crack Covid?", *Unheard* <https://unherd.com/2020/04/can-your-smartphone-crack-covid/> (accessed 27 April 2020)

> infected individuals or hotspot locations in that calculation. It sends your identity and location directly to a server accessible by the police, who can use it to enforce the quarantine demanded by your colour status. Use of the app is not compulsory, but even local movement may be impossible without it.

The author suggests that the public appetite to share information from our phones for legitimate control/crisis purposes will be dulled if it becomes widely known how this data can leak into other control/surveillance arenas.

> The solution to the Bluetooth privacy problem is that the exchanging and storing of randomly generated codes will happen, not in an app, but securely within the operating system. Data will leave the device only for explicitly authorised uploading to an approved database. The only other interactions possible with external databases will be queries about matching numbers. The app could potentially export any risk scores it has calculated for you, but not the codes sent and received by Bluetooth.

However, she rightly identifies the political location of the personal data protection agenda:

> Automated alerts can't replace detailed contact tracing, as practised in South Korea and Singapore. But interview based contact-tracing is labour intensive. Contact-tracing tens of thousands of cases individually would be an immense task for a health service that can't even pick up every 111 call. However, a widely used app in conjunction with testing could be a workable compromise, reducing the transmission rate to a scale that the NHS can handle, while allowing people for whom the risk is acceptably low to return to work, and to a more normal life.
> How low a risk is acceptable, and how normal life should be, are political questions. No app can answer those.

In a recent paper published by the Berkman Klein Centre for Internet and Society, and the Health Ethics and Policy Lab[90], the authors identified a typology of digital public health tools devised to tackle the pandemic. Similar to the processes described in more detail above, the typology spotted proximity tracing, symptom checkers, quarantine compliance tools and flow modelling capacities (the latter which we see instead as analytical enhancements rather than surveillance technology). Particularly helpful is the paper's classification of 'legal and ethical' challenges posed by these innovations and their consequent data usage. Validity, accuracy and necessity, correspond with this papers introductory and prevailing interests in purpose and objective. Privacy, discrimination, public benefit and expiration are common to matters interrogated below. We have treated consent and voluntariness as inextricable from the legal authority for the regulatory impact of these technologies and as such seen then more as concerns when initiating expanded data access. Digital inequality and repurposing are at the heart of fairness considerations and our approach to transparency. The Berkman Klein paper

[90] Urs Gasser, Marcello Ienca, James Scheibner, Joanna Sleigh, Effy Vayena, *Digital Tools against Covid-19; Framing the ethical challenges and how to address them*, BERKMAN KLEIN CENTRE FOR INTERNET AND SOCIETY, AND THE HEALTH ETHICS AND POLICY LAB WORKING PAPER (2020) <https://arxiv.org/ftp/arxiv/papers/2004/2004.10236.pdf>

progresses to connect ethical principles (autonomy, beneficence, justice, non-malfeasance, privacy and solidarity)[91] with these identified challenges and from there offers some interesting general recommendations for the ethical use of such public health tools.

Massive collections of data could help curb the COVID-19 pandemic, but emergency measures, particularly those that remain in place after the crisis has been contained, if they neglect civil rights and citizen dignity concerns then public trust will be a casualty. Best practices in surveillance and mass data use need to be identified along with responsible data-collection and data-processing standards at a global scale.

The crisis circumstances that the world is facing because of the COVID-19 are being used to justify some of these programmes in the short term. Some of these immediate measures confronting the health crisis have been strongly focused on surveillance, and even though there is a debate whether tracing is surveillance in the narrow sense. At the same time, it is equally important to consider the ethical challenges associated in the medium and long term for data subjects posed by any extension of data storage and use beyond emergency measures. Regardless of the nature of the programmes – whether public, private, permanent or temporal – all tracing initiatives should question the responsible collection and treatment of personal data for the ultimate purpose of the safety of mankind without sacrificing the human dignity of data subjects.

This section identifies these ethical challenges and potential risks in the short term, but also in the expanded or permanent use of the technology and applications of personal data for surveillance.

1. Public interest versus individual rights

These surveillance programmes are based on reasons related to public interest in controlling the spread of the COVID-19 pandemic. Those reasons require clear public enunciation. As the scale and severity of the COVID-19 pandemic rises to the level of a global public health threat[92] justifying restrictions on certain rights,[93] then causal relations between threat, control policy and intended outcomes require monitoring. Indeed, under the International Covenant on Economic, Social and Cultural Rights, which most countries have adopted, individuals have the right to "the highest attainable standard of physical and mental health." Governments are obligated to take effective steps for the "prevention, treatment and control of epidemic, endemic, occupational and other

[91] In other work soon to be published CAIDG has researched the operational accessibility, relevance and applicability of such high order ethical concepts and concedes that there are significant problems with the translation of this language into practical applications on front-line decision making – see Findlay & Seah (forthcoming) 'An Ecosystem Approach to AI Ethical Data Use; Research reflections'

[92] World Health Organization, "Coronavirus disease (COVID-19) Pandemic" <https://www.who.int/emergencies/diseases/novel-coronavirus-2019> (accessed 6 April 2020)

[93] For instance, such as those that result from the imposition of quarantine or isolation limiting freedom of movement. See Andrea Salcedo, Sanam Yar and Gina Cherelus, "Coronavirus Travel Restrictions, Across the Globe", *The New York Times* (15 April 2020) <https://www.nytimes.com/article/coronavirus-travel-restrictions.html> (accessed 7 April 2020)

diseases."[94] Concomitantly, careful attention to human rights such as non-discrimination and ethical principles like transparency and respect for human dignity can align with an effective control response even in the turmoil and disruption that inevitably results in times of crisis, when the urgent need to protect health dominates discussions of potential harm to other individual rights.

The responsible use of data in surveillance and tracing programmes should factor in the protecting of personal data even in emergency circumstances, such as the fight against COVID-19.[95] Some regulatory framework and flagged specific articles of the General Data Protection Regulation provide the legal grounds for processing personal data in the context of epidemics. For example, Article 9 allows the processing of personal data "for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health," provided such processing is proportionate to the aim pursued, respects the essence of the right to data protection and safeguards the rights and freedoms of the data subject. This means that data collection must be proportional to the seriousness of the public-health threat, be limited to what is necessary to achieve a specific public-health objective and be scientifically justified.

Many of the measures implemented by governments are based on extraordinary powers, only to be used temporarily in emergencies that allow government to disregard to some extent certain applicable laws, such as privacy protection provisions. In other instances, legal authority rests on permanent infectious diseases legislation but these are only to be activated in crisis context (see the Singapore example). Some forms of authority, for instance, use exemptions in data protection laws to share data.[96] Most of these measures

[94] See United Nations Human Rights, Office of the High Commissioner, International Covenant on Economic, Social and Cultural Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 3 January 1976, in accordance with article 27. Available at: https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx Additionally, the United Nations Committee on Economic, Social and Cultural Rights, which monitors state compliance with the covenant, has stated that: "The right to health is closely related to and dependent upon the realization of other human rights, as contained in the International Bill of Rights, including the rights to food, housing, work, education, human dignity, life, non-discrimination, equality, the prohibition against torture, privacy, access to information, and the freedoms of association, assembly and movement. These and other rights and freedoms address integral components of the right to health." See United Nations, Office of the Human Rights Commissioner, "CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)" (11 May 2000) <https://www.refworld.org/pdfid/4538838d0.pdf> (accessed 27 April 2020)

[95] The European Data Protection Board coincides with this approach. See "Statement on the processing of personal data in the context of the COVID-19 outbreak", *European Data Protection Board* (20 March 2020) <https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en> (accessed 7 April 2020)

[96] On March 16, it was reported that Korean telecommunication companies and credit card companies were sharing data to the government to assist tracking the movement of its citizens. It followed reports from earlier in the month that the government had launched an app to monitor citizens on lockdown to help contain the outbreak. Texts messages sent by health authorities and local district offices were also reportedly exposing an avalanche of personal information and are fuelling social stigma. See Kim Yeon-Ji, "세계가 놀란 확진자 동선 추적 '통신과 금융 인프라' 덕분 출처", *IT Chosun (16 March 2020)* http://it.chosun.com/site/data/html_dir/2020/03/14/2020031400735.html (accessed 27 April 2020); "South Korea: App monitors and enforces patient lockdown", Privacy International (6 March 2020) <https://www.privacyinternational.org/examples/3449/south-korea-app-monitors-and-enforces-patient-lockdown> (accessed 27 April 2020), Nemo Kim, "'More scary than coronavirus': South Korea's health

claim to be temporary, necessary, and proportionate. However, largely they have not addressed ethical issues so far.

The COVID-19 situation is not the first health crisis where public safety reasons were advanced to restrict individual rights, especially related to data protection and the responsible use of data. In 2014, privacy concerns urged the GSM Association[97] to issue guidelines on the protection of privacy in the use of mobile-phone data for responding to the Ebola outbreak.[98] In the present crisis similar concerns emerge about the secondary use of public health control data. There have been reports that China's digital epidemic control might have exacerbated stigmatisation and public mistrust.[99]

2. Individual dignity

Human dignity is a leading principle in public health ethics.[100] Health data is considered sensitive data in most jurisdictions meaning that data processors in this context are subject to particularly strict rules.[101] During previous public health crises, people with diseases and their families have often faced discrimination and stigma.[102] For instance, people living with HIV in Kenya, South Africa, the Philippines, and the United States faced discrimination due to their HIV status and have been prevented from accessing health care, getting jobs, and attending school.[103] Likewise, the stigma against survivors of Ebola in West Africa, in some cases, had led to eviction, loss of employment, abandonment, violence, and other consequences.[104] Since the coronavirus outbreak at the beginning of 2020, a number of countries have documented bias, racism, xenophobia, and

---

alerts expose private lives", *The Guardian UK* (6 March 2020) <https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives> (accessed 27 April 2020)

[97] An industry organization that represents the interests of mobile-network operators worldwide.

[98] Groupe Speciale Mobile Association, "GSMA Guidelines on the Protection of Privacy in the Use of Mobile Phone Data for Responding to the Ebola Outbreak", GSMA (19 Nov 2014), <https://www.gsma.com/mobilefordevelopment/resources/gsma-guidelines-on-the-protection-of-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-ebola-outbreak/> (accessed 27 April 2020)

[99] Marcello Ienca and Effy Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic", *Nature Medicine* (27 March 2020), <https://www.nature.com/articles/s41591-020-0832-5> (accessed 2 April 2020)

[100] Sebastian F. Winter and Stefan F. Winter, *Human Dignity as Leading Principle in Public Health Ethics: A Multi-Case Analysis of 21st Century German Health Policy Decisions*, INTERNATIONAL JOURNAL OF HEALTH POLICY AND MANAGEMENT VOLUME 7, ISSUE 3 (2018) Pg. 210-224. Available at: http://www.ijhpm.com/article_3374.html

[101] Jenna Mäkinen, *Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things*, INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 24.3 (2015), Pg. 262-277.

[102] "Human Rights Dimensions of COVID-19 Response", Human Rights Watch (19 March 2020), <https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response> (accessed 6 April 2020)

[103] Ibid.

[104] Emma Sacks, *Stigma and Ebola survivorship in Liberia: Results from a longitudinal cohort study*, PLOS ONE 13-11 (2018), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6261413/; Kelly JD, *Ebola virus disease-related stigma among survivors declined in Liberia over an 18-month, post-outbreak period: An observational cohort study,* PLOS NEGLECTED TROPICAL DISEASES. 13-2 (2019), available at: https://www.ncbi.nlm.nih.gov/pubmed/30811388

discrimination against people of Asia, from Asia in North world settings, and more recently against foreigners in Asian countries like China.[105]

South Korean authorities believe that 63 percent of the 7,300 confirmed cases in the country as at 7 March 2020[106] attended services held by the Shincheonji Church of Jesus in the city of Daegu or had contact with attendees.[107] In a statement, the church reported 4,000 incidents against congregants since the outbreak, including termination of employment, workplace bullying, domestic persecution, and labelling, and the church was blamed as the leading reason of the COVID-19 outbreak.[108] Moreover, public health alerts around the virus may not have adequately protected the privacy of individuals with the virus.[109] Some tracing programmes have even led to the discovery of extramarital affairs.[110]

Such discrimination based on presumed spread of the virus may have serious consequences for human dignity. Respect for the integrity of one's personal data is indeed an integral part of human dignity. Depending on what position one takes with respect to a philosophical anthropology, there follow different views about human dignity, and hence different ways of defending personal integrity in terms of privacy or otherwise.[111] Some may say that privacy is a luxury for the rich west, but the integrity of our personality and how it is represented when it is reduced to digitised formats cannot be denied as a universal concern for human dignity.

---

[105] Incidents include physical attacks and beatings, violent bullying in schools, angry threats, discrimination at school or in workplaces, and the use of derogatory language in news reports and on social media platforms, among others. Since January, media have reported alarming incidents of hate crimes in the United Kingdom, the US, Spain, and Italy, among other countries, targeting people of Asian descent, apparently linked to COVID-19. Quentin Fottrell, "'No Chinese allowed': Racism and fear are now spreading along with the coronavirus", *MarketWatch* (3 February 2020), <https://www.marketwatch.com/story/no-chinese-allowed-racism-and-fear-are-now-spreading-along-with-the-coronavirus-2020-01-29> (accessed 6 April 2020); Ang Hwee Min, "Singaporean student in London says he was assaulted after reacting to COVID-19 comments", *Channel News Asia* (3 March 2020), <https://www.channelnewsasia.com/news/singapore/singaporean-student-london-covid-19-attack-racist-jonathan-mok-12494174> (accessed 6 April 2020)

[106] Korea Centers for Disease Control and Prevention (KCDC), Korea website <https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030&act=view&list_no=366485&tag=&nPage=1> (accessed 27 April 2020)

[107] "Human Rights Dimensions of COVID-19 Response", *Human Rights Watch* (19 March 2020), <https://www.hrw.org/news/2020/03/19/human-rights-dimensions-covid-19-response> (accessed 6 April 2020)

[108] Raphael Rashid, "Being Called a Cult Is One Thing, Being Blamed for an Epidemic Is Quite Another", *The New York Times* (9 March 2020), <https://www.nytimes.com/2020/03/09/opinion/coronavirus-south-korea-church.html?auth=login-email&login=email> (accessed 27 April 2020)

[109] "Coronavirus privacy: Are South Korea's alerts too revealing?", *BBC* (5 March 2020), <https://www.bbc.com/news/world-asia-51733145> (accessed 6 April 2020)

[110] One recent alert concerned a woman, aged 27, who works at the Samsung plant in Gumi. It said that at 11:30 at night on 18 February she visited her friend, who had attended the gathering of religious sect Shincheonji, the single biggest source of infections in the country. "Coronavirus privacy: Are South Korea's alerts too revealing?", *BBC* (5 March 2020), <https://www.bbc.com/news/world-asia-51733145> (accessed 6 April 2020)

[111] Luciano Floridi, On Human Dignity as a Foundation for the Right to Privacy, PHILOSOPHY & TECHNOLOGY 29, 307–312 (2016), available at: https://doi.org/10.1007/s13347-016-0220-8

Moreover, some governments and private organisations are also working together to find ways back to *pre-virus normality* by relieving social distancing lockdowns and allowing some workers to go back into the workforce more quickly. These organisations are currently studying how many people are already immune to the COVID-19 virus,[112] and based on immunity status, issue an "immunity passports".[113] This approach should not be confused with a pre-emptive tracing initiative, but if implemented it would determine a different status and liberties among citizens on the basis of assumed reduced risk through anti-body protection. Non–passport holders would have their civil liberties and work opportunities constrained because of a higher risk determination. Those citizens that are considered to have the antibodies to fight the virus would be authorised to escape lockdowns and go back to previously held employment and socialising activities. If widely implemented, the 'passport' could be a starkly qualified step to engaging in a pre-pandemic society based on a discriminatory assessment of re-infection risk.[114] China is presently implementing a less hard-edged scheme where individuals seeking to travel in the country must obtain and display a health certification certificate, on their mobile devices.

So far governments and private organisations working on these segregation initiatives do not appear to be addressing the challenges related to discrimination, fairness or even if these initiatives would be constitutional or in violation of international human rights instruments. Against any confidence in such segregation initiatives, the World Health Organisation has stated that there is no sufficient evidence about the effectiveness of antibody-mediated immunity to guarantee the accuracy of an "immunity passport" or "risk-free certificate."[115] People who assume that they are immune to a second infection because they have received a positive test result may ignore public health advice at other levels and thereby engage in more risky behaviours on the assumption that they cannot be re-infected. The use of such certificates could therefore increase rather than guard against the propensity for continued transmission. As new evidence becomes available, the World Health Organisation will update their statement on anti-body protections.[116] Nonetheless, organisations and governments progress with immunity passports

3. Transparency

[112] Of course, this concept of immunity relies on the premise of protection against re-infection through possessing anti-bodies. There is science that takes a contrary view and argues there is no universal guarantee against re-infection.

[113] Kate Proctor, Ian Sample and Philip Oltermann, "'Immunity passports' could speed up return to work after Covid-19", *The Guardian* (30 March 2020) <https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work-after-covid-19> (accessed 4 May 2020)

[114] Jayakrishna Ambati, Balamurali Ambati, Benjamin Fowler, "Beware of Antibody-based COVID-19 'Immunity Passports'", *Scientific America* (28 April 2020) <https://blogs.scientificamerican.com/observations/beware-of-antibody-based-covid-19-immunity-passports/> (accessed: 4 May 2020)

[115] "Immunity passports in the context of COVID-19", World Health Organisation (24 April 2020) <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19> (accessed> 4 May 2020)

[116] "Immunity passports in the context of COVID-19", World Health Organisation (24 April 2020) <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19> (accessed> 4 May 2020)

Some technologies operate with little transparency in how data collected from different data points are processed, cross-checked and reused for surveillance purposes. For example, Alipay Health Code, an Alibaba-backed government-run app that supports decisions about who should be quarantined for COVID-19, also seems to share information with the police.[117] Because of the emergency, conventional data agreements to regulate responsible and accountable data use might be bi-passed, or overtaken by new and undeclared sharing arrangements so the public has little opportunity to understand how data is being used or demand appropriate checks and balances for accountability. While the state in times of crisis claims wider personal information and access, is the same confidence transferred to private companies turning over their location data to governmental agencies unless the data-subject provide was originally made fully aware of the use of the data, having trusted the data would be used as specified in any open and debated data agreement? In this manner the responsible use of data is directly correlated with transparency in the use of data, flowing on to the need to protect freedoms of movement, association, and anonymity.

Transparent public communication in relation to data processing for the common benefit is a characteristic of democratic state governance. With this in mind, data-processing agreements, where they have been crafted in an environment of democratic transparency, should disclose which data are transmitted to third parties and for which purpose.[118] Such transparency is even more important in countries such as the US, where the private sector dominates in developing the apps from which to share the resultant personal information with the government to control the virus, and where the countervailing protections of individual liberties are mandated constitutionally.[119] Some companies already share aggregate data, but it would be new for Google and Facebook to openly mine user movements on this scale on behalf of the government. The data collected would show patterns of user movements. It would need to be cross-referenced with data on testing and diagnoses to show how behaviour is affecting the spread of the virus. That said, Apple and Google have just announced an unprecedented data sharing initiative with little detail on the manner in which it should be accountable.[120]

4. Avoiding Biases

[117] Mozur, P., Zhong, R. & Krolik, A. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", *The New York Times* (1 March 2020), <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html> (accessed 6 April 2020)

[118] Marcello Ienca and Effy Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic", *Nature Medicine* (27 March 2020), <https://www.nature.com/articles/s41591-020-0832-5> (accessed 2 April 2020)

[119] Will Knight, "The Value and Ethics of Using Phone Data to Monitor Covid-19", *Wired* (18 March 2020), <https://www.wired.com/story/value-ethics-using-phone-data-monitor-covid-19/> (accessed 2 April 2020)

[120] Apple and Google are jointly developing technology to alert people if they have recently come into contact with others found to be infected with coronavirus. Their contact-tracing method would work by using a smartphone's Bluetooth signals to determine to whom the owner had recently been in proximity for long enough to have established contagion a risk. See Leo Kelion, "Coronavirus: Apple and Google team up to contact trace Covid-19", *BBC News* (10 April 2020) <https://www.bbc.com/news/technology-52246319> (accessed 27 April 2020); Patrick Howell O'Neill, "How Apple and Google are tackling their covid privacy problem", *MIT Technology Review* (14 April 2020) <https://www.technologyreview.com/2020/04/14/999472/how-apple-and-google-are-tackling-their-covid-privacy-problem/> (accessed 27 April 2020)

Following on from considerations of individual dignity being complemented by transparency, bias in data analysis, particularly as it applies to discriminatory risk interpretations of particular demographics is essential. There is nothing new in the challenge of data bias particularly where identification technology draws discriminatory conclusions on race and gender. In a pandemic it could however lead to life threatening discrimination and social exclusion, which will confirm xenophobic tendencies long after the crisis has receded. Avoiding biases in data collection and data processing is a particularly important consideration for situation such as COVID-19. Given the global spread of communicable diseases, there is both contemporary and historical precedent for improper government containment efforts driven by bias based on nationality, ethnicity, religion, and race—rather than facts about a particular individual's actual likelihood of contracting the virus, such as their travel history or contact with potentially infected people.[121] Against this experience, it is necessary to ensure that any automated data systems used to contain COVID-19 do not erroneously identify members of specific demographic groups as particularly susceptible to infection.[122] Insufficient or ineffective de-identification and biases in datasets can become major causes of distrust in public-health services.

Another ethical challenge linked to biases relates to the use of certain technologies that would be controversial in other circumstances. Such is the case with facial recognition. Clearview, a company that has built a vast facial recognition database using images scraped from the web, is reportedly talking to state officials about using its system to help trace those who have been in contact with coronavirus patients. Other companies are pitching tools for tracking the outbreak by mining social media content, in an atmosphere of market competition.[123]

Computer scientists have shown that facial recognition has greater difficulty differentiating between men and women the darker their skin tone. A woman with dark

---

[121] Demonising outsiders has proved to be common during pandemics. In the United States, existing anti-Asian prejudice fed on the disease's Chinese origin. When lumber yard proprietor Wong Chut King died of suspected plague in San Francisco in 1900, the authorities forcibly quarantined Chinatown, roping it off and surrounding it with police. Restrictions targeted ethnicity, not the likelihood of contact with the disease – white people were allowed to leave while Chinese people were contained. During the 1890s, a typhus outbreak on an immigrant ship led to the detention of 1,200 Russian Jews, and well into the 20th century new arrivals at Ellis Island faced segregation based on suspicion of infection. See Caroline Rance, "Demonising outsiders and stoking racial tensions: the dark history of quarantine practices", *History Extra, BBC History Magazine* (12 March 2020), <https://www.historyextra.com/period/modern/quarantine-plague-coronavirus-covid-racism-history-segregation-china-wuhan-deaths-leprosy/> (accessed 27 April 2020)
Another example of these demonization occurred during the plague outbreak. One of the best documented social outcomes of the plague in late-medieval Europe was the violence, often directed at Jews, who were accused of causing plague by poisoning wells. See Hanna Marcus, "What the Plague Can Teach Us About the Coronavirus", *New York Times* (1 March 2020) <https://www.nytimes.com/2020/03/01/opinion/coronavirus-italy.html> (accessed 27 April 2020)

[122] Matthew Guariglia and Adam Schwartz, "Protecting Civil Liberties During a Public Health Crisis", *Electronic Frontier Foundation* (10 March 2020) <https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis> (accessed 2 April 2020)

[123] Louise Matsakis, "Scraping the Web is a Powerful Tool. Clearview AI Abused It.", *WIRED* (25 January 2020) <https://www.wired.com/story/clearview-ai-scraping-web/> (accessed XXYY)

skin is much more likely to be mistaken for a man.[124] This limitation could lead to people of colour being wrongly identified as potential carriers.

5. Data aggregation

Gaining access to data from personal devices for contact tracing purposes, for example, can be justified if it occurs within specific bounds, has a clear purpose—e.g., warning and isolating people who may have been exposed to the virus—and other minimally invasive alternatives are not suitable —e.g., using anonymised mobile positioning data.[125]

Nonetheless, aggregate, anonymised location data is already made available to researchers by Google, Facebook, Uber, and cell phone companies. There is a history of such forms of surveillance in health crises. Researchers used data from cell phones pinging nearby towers to predict the spread of malaria in Kenya. That data was accurate within a few hundred meters. The data collected by phone operating systems and apps, which is often available to Google and Facebook, is typically more accurate. It is important to ensure that the data collected cannot be reversed engineered to track people for non-crisis purposes. Facebook already provides data for modelling disease spread via a project called Data for Good.[126]

Moreover, data aggregation is not necessarily a safe harbour for data protection. An ethical approach is needed for these type of surveillance especially if considering that any contact-tracing app would need to be used by more than half the total population to be effective.[127] It is important to avoid the creating of a tool that enables large-scale data collection on the population. Along these lines, more than 300 academics warned the National Health Services in England about solutions that allow reconstructing invasive information about the population. Those should be rejected from design.[128]

---

[124] Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH 81:1–15, CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (2018), available at: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

[125] Marcello Ienca and Effy Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic", *Nature Medicine* (27 March 2020), <https://www.nature.com/articles/s41591-020-0832-5> (accessed 2 April 2020)

[126] Will Knight, "The Value and Ethics of Using Phone Data to Monitor Covid-19", *Wired* (18 March 2020), <https://www.wired.com/story/value-ethics-using-phone-data-monitor-covid-19/> (accessed 2 April 2020); Amy Wesolowski et.al., *Quantifying the impact of human mobility on malaria*, SCIENCE 338(6104), Pg. 267–270 (2012), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3675794/: Facebook Data For Good, Disease Prevention Maps <https://dataforgood.fb.com/tools/disease-prevention-maps/> (accessed 27 April 2020)

[127] Oxford University, "Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown" (16 April 2020) <https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown> (accessed 27 April 2020).

[128] Alex Hern, "Digital contact tracing will fail unless privacy is respected, experts warn", *The Guardian UK* (20 April 2020) < https://www.theguardian.com/world/2020/apr/20/coronavirus-digital-contact-tracing-will-fail-unless-privacy-is-respected-experts-warn> (accessed 28 April 2020)

6. Expiration[129]

There is a key difference as we see it between transparency and explainability. In the Singapore example, the government has done much to empirically reveal the statistics that arise from tracing and tracking. But one might say there is an absence of explaining what these mean beyond the government's demographic categories of infection percentages. It might be considered not in their wider social engineering interests for some governments to stop these surveillance methods after crisis justifications have diminished. As in other major emergencies in the past, there is a hazard that the data surveillance infrastructure we build to contain COVID-19 may long outlive the crisis it was intended to address. The government and its corporate co-operators should be pressured to roll back any invasive programs created in the name of public health after crisis has been contained.[130] Obviously if civil society is to take on this role it needs to know how it is surveilled and where personal data ends up.

The Virus might be a feature of global epidemiology for some time to come, and these surveillance programmes could be used for predicting the new outbreaks, thereby arguing for their retention in terms of original purpose. But this must be put against other serious respiratory outbreaks that are seasonal, deadly, but do not advocate for such intrusive personal surveillance. Timetables for expiration at this stage are difficult to set but the importance of the policy objective can be presently agreed. The data of the previous outbreak especially related to how people responded to the measures adopted may be very important if the virus dies down but then spikes again. For instance, if social distancing has a major impact on the rate of spread, then it could be used to reduce infections as a medium term strategy.[131] Thus, if the surveillance mechanisms are to remain active for prevention purposes, it is important to regularly revisit the initial terms of the emergency exercise, and, in particular, its limited and contained health objectives. Simply to have this data as a stalking horse for all kinds of other social control preferences denies the initial emergency justifications and endangers their acceptance if they become a common call for social control and many other forms.

7. Explainability

If the government or a private company seek to limit a person's rights consequent on a surveillance programme (for example, to quarantine them based on the system's conclusions about their relationships or travel), in some jurisdictions[132] the data subject

---

[129] This topic is included as an important challenge not based on some utopian reflection that with the cessation of crises responsible for mass personal data generation and sharing, that data will vanish and the technologies responsible for it, will fall silent. Rather, the point as we see it relates to 'sunset' triggers that can be built into the technology and the life of the data, and firewalls that will make mass sharing more difficult once certain conditions are absent, that should be built-in to the surveillance strategies so that expiration beyond the crisis not some existential debate but a mechanical consequence.

[130] Matthew Guariglia and Adam Schwartz, "Protecting Civil Liberties During a Public Health Crisis", *Electronic Frontier Foundation* (10 March 2020) <https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis> (accessed 2 April 2020)

[131] Aimee R. Taylor et al., *Quantifying connectivity between local Plasmodium falciparum malaria parasite populations using identity by descent*. PLoS GENETICS. 13(10):e1007065 (2017), available at: https://journals.plos.org/plosgenetics/article?id=10.1371/journal.pgen.1007065

[132] For example in Europe under the General Data Protection Regulation.

should have the opportunity for timely and fair challenging of these conclusions and limits.[133] Moreover, explainability is a guiding principle within most if not all the ethical data use guidelines that companies and governments have published.[134] Hence, the results of big data and AI surveillance initiatives in a health crisis should be no less explainable in order to meet minimal universal ethical standards.

Having identified broad areas of potential ethical and regulatory challenge in the COVID-19 crisis context it is informative to shift into considerations of similar challenges posed in other sectors using surveillance for control purposes.

8. Anxiety Governance

The COVID-19 crisis has created a climate of fear and uncertainty in many contexts. In public mental health terms, the main psychological impact to date is elevated rates of stress or anxiety.[135] Personal physical safety prompts a willingness to compromise individual protections and liberties. It would also introduce notions of perverse citizenship, where it is good to comply, risking discrimination and social rejection if one does not. We call this an "indirect compulsion", seen in some political parlance as soft compliance or nudging. However, in the desire to comply through good citizenship/bad citizen tensions, citizens may not be aware that engagement with mapping and tracing appss could be used to extend emergency measures beyond the crisis, an outcome that many 'good citizens' would oppose.

This strategy seems to be working for governments in the context of the COVID-19 crisis to implement control tools that under different circumstances citizens will not be willing to use. For instance, in Australia, the government has already been circulating mas text messages and marketing campaigns to coordinate public action in dealing with COVID-19. This incentivises the adoption of the contact tracing app. Text-based nudges[136] can make salient the public gains from mass adoption, thereby appealing to social norms and peer pressure in further encouraging app adoption.[137] Texts could also make people aware

[133] Matthew Guariglia and Adam Schwartz, "Protecting Civil Liberties During a Public Health Crisis", *Electronic Frontier Foundation* (10 March 2020) <https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis> (accessed 2 April 2020)

[134] Adam Nagy and Jessica Fjeld, "Principled Artificial Intelligence Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI", *Berkman Klein Center for Internet & Society at Harvard University* (15 January 2020), <https://cyber.harvard.edu/publication/2020/principled-ai> (accessed 27 April 2020)

[135] "Mental Health and COVID-19", *World Health Organization* <http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/novel-coronavirus-2019-ncov-technical-guidance/coronavirus-disease-covid-19-outbreak-technical-guidance-europe/mental-health-and-covid-19> (accessed 29 April 2020)

[136] Cass R. Sunstein, *The Meaning of Masks*, FORTHCOMING JOURNAL OF BEHAVIORAL ECONOMICS FOR POLICY (2020). Available at: https://ssrn.com/abstract=3571428

[137] David P. Byrne, Richard Holden and Joshua B. Miller, "The big nudge: here's how the government could spread its coronavirus tracing app far, fast and wide", *Crikey Independent Inquiry Journalism* (27 April 2020) <https://www.crikey.com.au/2020/04/27/covidsafe-public-nudge/> (accessed 29 April 2020); The Minister of Health in Austtralia stated in a press conference in which the app was launch that "as part of our work in supporting those doctors and nurses we will be releasing the CovidSafe app, and the CovidSafe app is about assisting, finding those cases which might be undiagnosed in the community, helping people get earlier treatment, helping people to have earlier diagnosis, and to ensure that our doctors

of the extent to which others in their community, or neighbouring communities, have downloaded the app; research suggests that unfavourable social comparisons would motivate app adoption.[138]

National border closures have become the norm. In some political and cultural contexts these protectionist policies determined on citizenship and foreigner exclusion may have proved effective in limiting the virus spread but they risk exacerbating pre-existing prejudices against the outsider and making any orderly resumption of migration, refugee relief and even international tourism more problematic.

In some countries such as the USA a populist backlash by small groups of nationalist protesters has portrayed the 'right to work', and the countervailing restrictions on movement and association as threats to constitutional liberties in the same way that gun control initiatives are represented as non-constitutional. In these examples of polarised public opinion, it is easy to see how actions by the state originally designed as health control measures may dangerously dovetail into anxieties that go well beyond the virus and its reduction. Such anxiety progression (and aggravation) risks diverting attention from the central issues of concern that arise out of surveillance and mass data-sharing, making action to prevent negative consequences from these specific interventions all that harder to attain.

VI. SIMILAR USE CASES – THE FINANCIAL SECTOR APPROACH TO DATA-DRIVEN SURVEILLANCE

Data-driven surveillance is commonly used in other sectors on a daily basis, not only in times of emergencies. We will explore two cases from the financial sector where we may be able to draw some policy recommendations for the responsible use of data in surveillance programmes of COVID-19. Even though we will refer to machine leaning and AI implications and challenges as these technologies are used for data-driven surveillance applications in the financial sector, some of the challenges in relation to ethics, data protection and data usage extrapolate to other type of data-driven surveillance mechanisms. Likewise, the experience from other sectors, such as the financial sector, with data-driven surveillance, faces similar challenges.

1. Regtech - Anti-money laundering, know your customer and tracing fraudulent transactions

In recent years, especially after the 2008-2009 global financial crisis, financial institutions have been exploring ways of reducing operational costs and being more efficient. Therefore, the digital transformation processes of the fintech age have positively impacted compliance processes. In particular combating money laundering is an

---

and nurses, our health workers, our families and our friends are protected - and that will save lives and protect lives." "Press conference about the COVIDSafe app launch", *Ministers Department of Health* (26 April 2020) <https://www.health.gov.au/ministers/the-hon-greg-hunt-mp/media/press-conference-about-the-covidsafe-app-launch> (accessed 29 April 2020)

[138] Per Engström, Katarina Nordblom, Henry Ohlsson, and Annika Persson, *Tax Compliance and Loss Aversion*, AMERICAN ECONOMIC JOURNAL: ECONOMIC POLICY 2015, 7(4): 132–164 <https://pubs.aeaweb.org/doi/pdf/10.1257/pol.20130134>

enormous task, and it comes with substantial costs and risks, including but not limited to regulatory, reputational and financial risks. Hence, industry participants and regulators welcome new ways to sharpen surveillance on an ongoing basis for the purposes of effectively satisfying government financial transaction reporting requirements.

Banks have taken steps to work with different players in the *regtech*[139] ecosystem to combat money laundering using Machine Learning ("ML") and AI. Traditional ways of surveillance are less successful, resulting in large numbers of false positives (95% in some banks).[140] Additionally, since the global financial crisis, financial institutions are looking into ways of making their compliance much more efficient, making regtech very popular in recent years.[141]

Technology companies and banks are actively designing AI solutions and tools to better assess high risk jurisdictions, to identify potentially problematic or suspicious funds movements, and to refine the screening of Politically Exposed Persons ("PEP") and sanctioned individuals and/ or organisations. Regulators are also in agreement that such advanced technologies can and should be leveraged by banks to improve risk identification and mitigation.

Financial institutions also use regtech to analyse millions of documents and check details against 'blacklists' for the know-your-customer ("KYC") checks before the on-boarding account opening process begins. Particularly banks are increasingly using ML to rate the likelihood of a customer posing a financial crime risk, and as customers transfer money or make payments, firms use machine learning to identify suspicious activities and flag potential cases, so human analysts can focus on these specifically.[142]

These are some safeguards and limitations discussed in the financial industry on the matter in the context of digital transformation and especially the use of data-driven solutions:

---

[139] RegTech can be defined as the use of technological solutions to facilitate compliance with and monitoring of regulatory requirements. In recent legal doctrine, RegTech is almost unequivocally hailed as holding the promise of substantial gains in terms of increased efficiency and reduced risk of human errors and resulting administrative fines. See Veerle Colaert, *RegTech as a Response to Regulatory Expansion in the Financial Sector* (2018). Available at: https://ssrn.com/abstract=2677116, Douglas W. Arner, Janos Barberis, Ross P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, NORTHWESTERN JOURNAL OF INTERNATIONAL LAW & BUSINESS (2016), available at: https://ssrn.com/abstract=2847806

[140] Joshua Fruth, "Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states", *Reuters* (14 March 2018) <https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-moneylaundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV> (accessed 27 April 2020)

[141] Douglas W. Arner, Janos Barberis, Ross P. Buckley, *FinTech, RegTech and the Reconceptualization of Financial Regulation*, NORTHWESTERN JOURNAL OF INTERNATIONAL LAW & BUSINESS (2016), available at: https://ssrn.com/abstract=2847806

[142] Bank of England, Financial Conduct Authority, "Machine learning in UK financial services" (October 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf> (accessed 27 April 2020)

- *Human in the loop*: For the KYC tools, human analysts continue to play a decisive role in the process.[143] Once alerts are raised, analysts can narrow their focus to these more relevant sources. At the more advanced end, tools have the capacity to output a 'next step' for the analyst, who may agree or disagree with the decision. Firms say this helps improve the performance of the model because the system will adapt and refine its options on further use depending on the human decision.

- *Fairness and explainability*: Adherence to data protection policies, fair use of personal data and the legal right to explanation are important considerations in deciding on the scope of data used to train and operate the AI as well as outputs and information that can be shared by the AI. Financial institutions must be prepared to explain the details of the model, how it works, and to explain the decisions that the approach makes to avoid compliance breaches. Employing an army of data scientists is not enough – though likely highly skilled in technology, having the layer of financial crime domain expertise on top of that is essential in an intricate and highly-regulated field.[144]

  For transaction monitoring, the main complexity issues arise from the management of IT infrastructure and the oversight of data pathways and validation, according to the Financial Conduct Authority ("FCA").[145] Tools of a high technical complexity often combine a range of Machine Learning methods to draw insights on customers. The input data is of all structures,[146] and the explainability of the learning process is of great interest to firms deploying such tools[147] given that banks, in most jurisdictions, justify why a particular customer or transaction is flagged. Therefore, their interest to break down the unsupervised learning procedure of neural networks of a machine learning tool for transaction monitoring.

- *Transparency and auditability*: The ability to demonstrate and audit compliance is a cornerstone of the current anti-money laundering ("AML") framework — so the transparency of AI and its underlying algorithms is important. AI and machine

[143] Bank of England, Financial Conduct Authority, "Machine learning in UK financial services" (October 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf> (accessed 27 April 2020

[144] Chad Hetherington, "'Explainable AI': The Next Frontier in Financial Crime Fighting", *NICE* (25 Febriary 2019), available at: https://www.niceactimize.com/blog/explainable-ai-the-next-frontier-in-financial-crime-fighting-595/ (accessed 27 April 2020)

[145] Particularly in UK. Bank of England, Financial Conduct Authority, "Machine learning in UK financial services" (October 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf> (accessed 27 April 2020

[146] In computer science, a data structure is a data organization, management, and storage format that enables efficient access and modification. More precisely, a data structure is a collection of data values, the relationships among them, and the functions or operations that can be applied to the data. There are generally four forms of data structures: linear, tree, hash, graphs. See Mark McDonell, "Data Types and Data Structures, Integralist", Integralist (30 January 2019), available at: <https://www.integralist.co.uk/posts/data-types-and-data-structures/#data-structures> (acessed 13 April 2020)

[147] Bank of England, Financial Conduct Authority, "Machine learning in UK financial services" (October 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf> (accessed 27 April 2020

learning are broad fields with varying levels of complexity and transparency. At the more complex end of the spectrum, neural networks and deep learning may prove more difficult areas in which to build trust, when compared with more existing processes. At present, very few of the current AML solutions being trialed in banks have advanced beyond regression, decision trees and clustering due to these challenges.

- *Data quality and training*: Data quality is a major challenge for many financial institutions and often impacts the effectiveness and efficiency of AML controls. Projects need to assess data quality and its appropriateness for use by AI as part of the design and development phase, and also implement data management controls to monitor the ongoing data quality during operation and how model are trained. Recent cases in the financial industry have gone wrong already (mostly in credit scoring, not in AML).[148]

2. Suptech- Misconduct and Market Surveillance by Financial Regulators

Some financial regulators are using AI for market surveillance and fraud detection, which is also known as *suptech*.[149] For instance, the Australian Securities and Investments Commission ("ASIC") has been exploring the quality of results and potential use of Natural Language Processing ("NLP") technology to identify and extract entities of interest from evidentiary documents.[150] ASIC is using NLP and other technology to visualise and explore the extracted entities and their relationships. In order to fight criminal activities carried out through the banking system (such as money laundering).

The FCA performs network analysis on orders and executions data to construct webs of market participants and identify collusive behaviour indicating insider trading, while the Netherlands Bank ("DNB") employs a similar technique to link individuals sending funds to the same counterparties in high-risk jurisdictions along various routes.[151]

Market regulators can also use these techniques for disclosure and risk assessment. The US Securities and Exchange Commission ("SEC") staff leverages "big data" to develop text analytics and machine learning algorithms to detect possible fraud and misconduct. For investment advisers, the SEC staff compiles structured and unstructured data.

---

[148] Patrick Craig, "How to trust the machine: using AI to combat money laundering", *EY* (3 September 2019) <https://www.ey.com/en_in/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering> (accessed 27 April 2020)

[149] Suptech refers to the application of big data or artificial intelligence (AI) to tools used by financial authorities. See Simone di Castri, Stefan Hohl, Arend Kulenkampff and Jermy Prenio ,*The suptech generations*, FINANCIAL STABILITY INSTITUTE INSIGHTS ON POLICY IMPLEMENTATION NO 19, available at: https://www.bis.org/fsi/publ/insights19.pdf

[150] Jamie Smyth, "Australian regulators cautiously embrace AI to boost compliance", *Financial Times* (8 April 2019) <https://www.ft.com/content/33eb5934-4519-11e9-b168-96a37d002cd3> (accessed 27 April 2020)

[151] Suptech refers to the application of big data or artificial intelligence (AI) to tools used by financial authorities. See Simone di Castri, Stefan Hohl, Arend Kulenkampff and Jermy Prenio ,*The suptech generations*, FINANCIAL STABILITY INSTITUTE INSIGHTS ON POLICY IMPLEMENTATION NO 19, available at: https://www.bis.org/fsi/publ/insights19.pdf

Unsupervised learning algorithms are used to identify unique or outlier reporting behaviours – including both topic modelling and tonality analysis. The output from this first stage is then combined with past examination outcomes and fed into a second-stage, machine learning algorithm to predict the presence of idiosyncratic risks at each investment advisor.[152]

Despite the benefits that these early adopters are exploring by using technology in their surveillance processes, they also recognise challenges and risks of this type of surveillance. First, use of suptech without taking the necessary measures to address technical, data quality, legal, operational, reputational, resource, internal support and practical issues may expose supervisors to undue risks.[153] Moreover, although suptech can help identify potential issues and problems, human intervention is necessary to pursue further investigations and decide on a suitable course of action.[154] Second, according to the Financial Stability Institute, supervisory agencies also need to be cautious of a growing data-knowledge gap. On one hand, data availability, data quality and data storage facilities are improving rapidly, as are techniques for combining different data sources. On the other hand, data analytics may not be advancing at the same pace. It takes time to learn, develop and implement new technologies in supervision work. Agencies could make an assessment of data availability and to what extent data is being fully used in supervision work.[155]

CONCLUSION

For a paper like this written in the middle of a global health pandemic wherein governments and private companies worldwide are utilising AI-assisted surveillance, reporting, mapping and tracing technologies with the intention of slowing the spread of the virus, there is no simple conclusion. These technologies have capacity to amass personal data and share for community control and citizen safety motivations that empower state agencies and inveigle citizen co-operation which could only be imagined outside such times of real and present danger.

The paper has attempted some simple descriptive intentions in identifying and detailing tracking, tracing and surveillance technologies preferred in certain geo-political crisis contexts. This enterprise loosely employed the analytical device of extant crisis objectives, explaining their authority and process. As the descriptions developed from Singapore and China to survey (with the assistance of the attached appendix) tracing and quarantine priorities across the globe, the introduction of possible non-crisis connected

[152] The Financial Stability Board, Artificial intelligence and machine learning in financial services. Market developments and financial stability implications (2017), available at: https://www.fsb.org/wp-content/uploads/P011117.pdf

[153] Dirk Broeders and Jermy Prenio, *Innovative technology in financial supervision (suptech) – the experience of early users,* FINANCIAL STABILITY INSTITUTE INSIGHTS ON POLICY IMPLEMENTATION NO 9 (2018), available at: https://www.bis.org/fsi/publ/insights9.pdf

[154] Dirk Broeders and Jermy Prenio, *Innovative technology in financial supervision (suptech) – the experience of early users,* FINANCIAL STABILITY INSTITUTE INSIGHTS ON POLICY IMPLEMENTATION NO 9 (2018), available at: https://www.bis.org/fsi/publ/insights9.pdf

[155] Dirk Broeders and Jermy Prenio, *Innovative technology in financial supervision (suptech) – the experience of early users,* FINANCIAL STABILITY INSTITUTE INSIGHTS ON POLICY IMPLEMENTATION NO 9 (2018), available at: https://www.bis.org/fsi/publ/insights9.pdf

purposes for surveillance and containment were flagged. A more critical review of these challenges for integrity, dignity, freedom and civil liberty was the subject of the final section as it projected social engineering possibilities not serviced by crisis justifications.

With the purpose to raise awareness, and inspire the debate to shape better policies for the ongoing use of intrusive personal data use once crafted for emergency circumstances,, the paper addressed the general ethical challenges represented in such eventualities, covering broad concerns of privacy and data protection, to more expressly targeted issues of freedom of movement and association, confidence in data use for data purpose, trust in data sharing, and overall fairness. Likewise, the analysis reflects on other surveillance methods, outside the health context, where similar challenges have arisen.

In its developed form a later version of this paper will speculate on and offer suggestions regarding regulatory responses when faced with extended surveillance, tracking/tracing, public/private provider data sharing and any breakdown in personal data firewalls, or otherwise conventional aggregated data constraints.

Appendix A – Infrastructure application for surveillance and pre-emptive tracing in the COVID-19 emergency

Table 1. Tracing and surveillance initiatives in different jurisdictions

Country or region	Purpose	Level of abstraction	Method	Description
Europe	Contact tracing	Individual	Phone proximity	The Pan-European Privacy-Preserving Proximity Tracing uses Bluetooth for phone proximity tracing.
Indonesia	Contact tracing	Individual	Phone proximity	The government has developed an app called PeduliLindungi for proximity tracing
Iran	Contact tracing	Individual	Phone location	Individuals have been asked to download an app which predicts if users have COVID by asking them short questions about their health. The app also tracks location and other personal information.
Israel	Contact tracing	Individual	Phone location	The government uses data from telcos to trace close contacts
Israel	Contact tracing	Individual	Phone location	The government has developed at app called HaMagen (Hebrew for shield) for contact tracing
Norway	Contact tracing	Individual	Phone location; phone proximity	The Norwegian government and company Simula have built a voluntary app which tracks location and proximity.
Philippines	Contact tracing	Individual	Phone location	The government has developed at app called WeTrace for contact tracing.
Singapore	Contact tracing	Individual	Other	Manual tracing is conducted with verbal interviews, CCTV footage, and card usage.
Singapore	Contact tracing	Individual	Phone proximity	The government has developed an app called TraceTogether for proximity contact tracing.
South Korea	Contact tracing	Individual	Other	Manual tracing is conducted with verbal interviews, phone location tracking, CCTV footage, and card usage.

UK	Contact tracing	Individual	Phone proximity	The UK is developing a proximity tracing app.
US	Contact tracing	Individual	Phone proximity	Several proximity tracing apps are under development, such as Safe Paths, COVID Watch, and Corona Trace.
Argentina	Maintain quarantine	Individual	Phone location	Individuals entering the country and those who have violated quarantine have to install an app which tracks their location for 14 days.
Australia	Maintain quarantine	Individual	Other	Individuals who do violate quarantine may have surveillance devices installed in their home or be made to wear tracking devices. The Australian government has opted not to use phone-based location tracking.
Austria	Maintain quarantine	Aggregated	Phone location	Teleco A1 provided the government two days' worth of location data. The data was anonymised and could only be analysed in groups of more than 20. The data showed that citizens have reduced their social contact.
Bahrain	Maintain quarantine	Individual	Phone location	Individuals who test positive have to wear an electronic bracelet which connects to a mobile app to track their location.
Belgium	Maintain quarantine	Aggregated	Phone location	Three telcos are sharing information with the consulting firm Dalberg to analyse general movement trends.
Brazil	Maintain quarantine	Unclear	Phone location	Several city governments are tracking location data from phones.
China	Maintain quarantine	Individual	Other	Individuals in more than 200 cities have to download an app called "Alipay Health Code". Users are assigned a grade which determines whether they can enter various public places
Dubai	Maintain quarantine	Individual	Other	Traffic police scan vehicle license plates and cross-reference against a list of approved essential workers.
Ecuador	Maintain quarantine		Phone location	The government is tracking the location of phones to ensure that people are following isolation measures.
Germany	Maintain quarantine	Aggregated	Phone location	Telco Telekom is sharing location data with the government. The data is anonymised and aggregated to analyse general patterns of movement.

Hong Kong	Maintain quarantine	Individual	Phone location	Individuals under quarantines must wear electronic wristbands that pair with their phone and track their location.
India	Maintain quarantine	Individual	Phone location	Suspected cases received hand stamps detailing the date until which they must quarantine. Some individuals are being tracked using their mobile phones and personal data to help enforce quarantines.
Italy	Maintain quarantine	Unclear	Phone location	Vodafone has provided the government information about users location.
Poland	Maintain quarantine	Individual	Other	Individuals under quarantine have to send a picture of themselves at home, which is automatically matched against a previously submitted reference photo.
Russia	Maintain quarantine	Individual	Phone location	Individuals under quarantine are monitored with facial recognition and phone-based location tracking.
Singapore	Maintain quarantine	Individual	Phone location	Individuals who have been issued stay-home-notices are sent a text message. Clicking the link directs them to a website which checks their location.
South Korea	Maintain quarantine	Individual	Phone location	Individuals who have been told to stay home can download a "self-quarantine safety protection" app that monitors their location with GPS. The app also lets the person stay in touch with case workers.
Switzerland	Maintain quarantine	Aggregated	Phone location	Telco Swisscom will alert the federal government when more than 20 phones are gathered in a 100-square-meter area.
Taiwan	Maintain quarantine	Individual	Phone location	Individuals under quarantine have their phone locations monitored.
Thailand	Maintain quarantine	Individual	Phone location	Individuals arriving from high risk areas are given SIM cards to help the government track their location for 14 days.
Turkey	Maintain quarantine	Individual	Phone location	Individuals under quarantine have their phone locations tracked.
South Africa	Unclear	Unclear	Phone location	Telecom companies have agreed to give the government cell phone location data. The details of the program are unclear.

Source: Gershgorn, Dave. 'We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World'. OneZero, 9 April 2020. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9.