Regulating Personal Data Usage in COVID-19 Control Conditions

Mark Findlay[1], Nydia Remolina[23]

SMU Centre for AI & Data Governance Research Paper No. 2020/04

Abstract

As the COVID-19 health pandemic ebbs and flows world-wide, 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 and share personal data for community control and citizen safety motivations that empower state agencies and inveigle citizen co-operation which could only be imagined outside times of real and present personal 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 (provided that the technology can be shown to be fit for purpose)[4], the paper argues that this technological infrastructure for surveillance can have serious ethical and regulatory implications in the medium and long term when reflected against human dignity, civil liberties, transparency, data aggregation, explainability and other governance fundamentals. The paper commences with the case for regulation recognising crisis exigencies, after which it reiterates personal data challenges, then surveys policy and regulatory options to equitably address these challenges.

[1] Director, Centre for AI and Data Governance, Singapore Management University
[2] Research Associate, Centre for AI and Data Governance, Singapore Management University
The authors acknowledge the assistance of Loke Jia Yuan with research into discrimination, and sunset clauses.
[3] 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.
[4] As highlighted recent discussions surrounding smartphone tracing apps, with the necessity for high uptake proportions, particularly in regions where smart phone usage is not the norm, the achievement of the apps' purpose, even if compulsorily required, remains problematic.

Table of Contents

Introduction

Concern is growing about the potential for COVID-19 control technologies and resultant data sharing negatively impacting on civil rights, invading personal privacy, undermining citizen dignity through expansive data matching and ultimately providing opportunities for data use well beyond the brief of virus mitigation. Citizen trust may be another tragic victim of the pandemic, without appropriate and proportionate regulatory intervention.

This paper offers suggestions regarding effective and inclusive 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 deviations and distortion. In doing so, the paper explores personal data usage in the context of COVID-19 as a regulatory enterprise. Hence, the paper addresses four fundamental features influencing the ultimate regulatory decision and direction: why, when, where and what. Then the paper overviews challenges posed to personal data subject and concludes by presenting regulatory strategies addressing the challenges of data usage in COVID-19 control conditions.

PART 1. How to regulate data use?

In approaching any regulatory enterprise there are four fundamental features influencing the ultimate regulatory choice and direction:

Why – the simple answer is that because many of the health control technologies employed to fight the virus produce, use, store or disseminate personal data then this should not proceed without responsible governance.[5] But the matter is not so simple. Because of the risks to life and health posed by the virus, and that any personal claims over data are always contextual, this pandemic control situation for regulators necessitates balancing objective challenges to privacy and data integrity against individual and collective well-being. Regulatory balancing opens up another line of debate which characterises recent public resistance to the containment of liberties in movement and association.[6] Are the control justifications for employing personal data and restricting liberties valid, or indeed excessive?[7]

---

[5] Trix Muller, *Health apps, their privacy policies and the GDPR*, EUROPEAN JOURNAL OF LAW AND TECHNOLOGY VOL 10, NO 1 (2019) < http://ejlt.org/article/view/667/897>; Bobby Fung, In this time of the coronavirus, does personal data privacy get thrown out the window?, Withers World Wide (20 March 2020) <https://www.withersworldwide.com/en-gb/insight/in-this-time-of-covid-19-does-personal-data-privacy-get-thrown-out-the-window> (accessed 19 May 2020); European Patients Forum, The new EU Regulation on the protection of personal data: what does it mean for patients? (2018), <https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf>

[6] "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); European Union Agency for Fundamental Rights, *Coronavirus Pandemic in the EU - Fundamental Rights Implications,* Bulletin #1 (20 March 2020) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-coronavirus-pandemic-eu-bulletin_en.pdf> (accessed 18 May 2020); Becky Beaupre Gillespie, "In the fight against COVID-19, how much freedom are you willing to give up?" University of Chicago News (13 April 2020) <https://news.uchicago.edu/story/fight-against-covid-19-how-much-freedom-are-you-willing-give> (accessed 18 May 2020)

[7] Suzanne Nossel, "Don't Let Leaders Use the Coronavirus as an Excuse to Violate Civil Liberties, Foreign Policy", *Foreign Policy* (30 April 2020) <https://foreignpolicy.com/2020/04/13/governments-coronavirus-pandemic-

Thus, the *why* question becomes difficult to isolate from the consent, compliance, good-will or even reluctant acquiescence of the data subject.

When – again the simple answer is that the regulatory timetable should be inversely related to the retreat of the virus. But whether it is because of doubts about the science, the statistical modelling, or the quantification of tolerable harm,[8] only a brave or foolish person would put a date on this eventuality. In any case, when the emergency conditions are sufficiently relieved to return to considerations of conventional personal data protection may be more a political and economic, rather than a health sciences determination.[9] To avoid inconsequential deliberations over when is it safe enough to be concerned enough about personal data use, regulators can suggest it is more productive to get protections in place as we roll out and apply intrusive technologies.[10] This thinking accepts either that there is no crisis too great or no personal data too insignificant to obviate the need for regulatory oversight.

Where – again answered simply, wherever the data is produced, stored, accessed and used. Yet in the spirit that data has value for those on whose behalf we regulate, regulatory activity, its location and reach will depend on how much the regulatory recipient wants something to

---

civil-liberties/> (accessed 19 May 2020); Martin Bull, *Beating Covid-19: The problem with national lockdowns*, The London School of Political Science, EUROPP - European Politics and Policy Blog (26 March 2020) <https://blogs.lse.ac.uk/europpblog/2020/03/26/beating-covid-19-the-problem-with-national-lockdowns/> (accessed 18 May 2020)

[8] Bill Gardner, "Sage having 'heated arguments' over science of lockdown", The Telegraph (10 May 2020) <https://www.telegraph.co.uk/news/2020/05/10/sage-committee-split-heated-arguments-scientist-reveals/> (accessed 18 May 2020); Debashree Ray, Maxwell Salvatore, Rupam Bhattacharyya, Lili Wang, Shariq Mohammed, Soumik Purkayastha, Aritra Halder, Alexander Rix, Daniel Barker, Michael Kleinsasser, Yiwang Zhou, Peter Song, Debraj Bose, Mousumi Banerjee, Veerabhadran Baladandayuthapani, Parikshit Ghosh, Bhramar Mukherjee, *Predictions, role of interventions and effects of a historic national lockdown in India's response to the COVID-19 pandemic: data science call to arms*, MedRxiv (2020) <https://www.medrxiv.org/content/10.1101/2020.04.15.20067256v1>; Geofrey Musinguzi and Bennedict Oppong Asamoah, *The Science of Social Distancing and Total Lock Down: Does it Work? Whom does it Benefit?,* ELECTRONIC JOURNAL OF GENERAL MEDICINE 17(6) (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3571947>

[9] Scientific models are estimates, and scientists regularly disagree about different issues, methodologies, approaches. And, even in the hypothetical and rare scenario where they all agree, scientists can only tell politicians the conditions under which their models are likely to work, but they are not responsible for creating or implementing the models. Thus, scientists can provide evidence, but acting on that evidence requires political will and political decision-making. When it comes to policymaking, economic and political considerations tend to take precedence. Jana Bacevic, "There's no such thing as just 'following the science' – coronavirus advice is political", The Guardian UK (28 April 2020) <https://www.theguardian.com/commentisfree/2020/apr/28/theres-no-such-thing-just-following-the-science-coronavirus-advice-political> (accessed 18 May 2020)
In the context of the coronavirus disagreements among the scientific community are evident. For instance, epidemiologist Anders Tegnell advocates for implementing a no-lockdown strategy. He is the architect of Sweden's response to COVID-19. Primary and secondary schools, restaurants, cafés and shops are mostly open as normal in Sweden, with health authorities relying on voluntary social distancing and people opting to work from home. Richard Milne, "Architect of Sweden's no-lockdown strategy insists it will pay off", Financial Times (8 May 2020) <https://www.ft.com/content/a2b4c18c-a5e8-4edc-8047-ade4a82a548d> (accessed 18 May 2020)

[10] By "intrusive technologies" we mean any type of data-driven initiative that automatically collects and/or shares personal data that outside the crisis context of the pandemic data would likely be subject to limitations or protections.

be done and done now. At the risk of tokenism, there seems little doubt that the value of personal privacy is militated by access to private space, and familiarity with rights discourse.[11] A key strategy in the fight against the virus promoted by North World states[12] has been social distancing. The discriminatory resonance of that discourse for migrant workers confined in hostels, prisoners and mental health patients in secured facilities, residents in aged-care institutions, the poor in slums, and people living on the streets should not justify regulatory location only where personal data and individual liberties are actionable.

What – regulatory techniques range across a continuum of command and control to the least intrusive compliance formats.[13] Where any regulatory initiative sits on that continuum will depend on the urgency for a regulatory outcome, cooperation with or resistance against regulatory intent, and the extent to which regulatory needs can be quarterized from other unconnected or competing regulatory demands. This latter consideration is prominent when competing pressures exert to protect data or otherwise to enable access for different purposes and priorities. Another important determinant when choosing a preferred regulatory technology[14] is the extent to which regulatory recipients identify the need for behavioural change outcomes.[15] Take, for instance, the recently introduced 'safe entry' protocols which require that citizens wanting to gain access to designated private and public premises only may do so if they pass certain health screening, and provide automated identity

---

[11] Charles Raab and Benjamin Goold, *Protecting information privacy,* Equality and Human Rights Commission Research report 69 (2011) <https://www.equalityhumanrights.com/sites/default/files/research-report-69-protecting-information-privacy.pdf>. The rights discourse is present even in Asian countries that do not always include a "right to privacy" in their legal and constitutional regimes. Asian courts with the most developed privacy jurisprudence frequently use similar language to protect privacy. Courts have found privacy to be an implied right based on protections of dignity and autonomy interests, such as personality development and informational self-determination. In defining valid restrictions on the constitutional right of privacy, the courts have adopted strikingly similar legal tests. Graham Greenleaf, *The Right to Privacy in Asian Constitutions*, in THE OXFORD HANDBOOK OF CONSTITUTIONAL LAW IN ASIA, FORTHCOMING (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3548497>

[12] United States, Canada, the United Kingdom, all member states of the European Union, Russia, Israel, Japan, Singapore, South Korea, Australia, and New Zealand.

[13] Mark Findlay, *Corporate Sociability: Analysing Motivations for Collaborative Regulation*, RESEARCH COLLECTION SINGAPORE MANAGEMENT UNIVERSITY SCHOOL OF LAW 5-2014 (2014), ADMINISTRATION AND SOCIETY. 46, (4), 339-370 (2014) <https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=4001&context=sol_research>

[14] In talking of optional regulatory 'technologies' this refers to the style of regulation (both in substance and application), not to be confused with any technology against which regulation might be directed.

[15] Bernard Marr, COVID-19 Is Changing Our World – And Our Attitude To Technology And Privacy –Why Could That Be Dangerous?, Forbes (23 March 2020) <https://www.forbes.com/sites/bernardmarr/2020/03/23/covid-19-is-changing-our-world--as-well-as-our-attitude-to-technology-and-privacy-why-could-that-be-a-problem/#45c68cdd6dc1> (accessed 18 May 2020); Salma Khalik, "Coronavirus: Expect a new normal even if current circuit breaker measures are eased", The Straits Times Singapore (7 May 2020) <https://www.straitstimes.com/singapore/expect-a-new-normal-even-if-current-measures-are-eased> (accessed 18 May 2020); 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); Shruti Bhargava, Courtney Buzzell, Christina Sexauer, Tamara Charm, Resil Das, Cayley Heller, Michelle Fradin, Grimmelt, Janine Mandel, Kelsey Robinson, Abhay Jain, Sebastian Pflumm, Anvay Tewari and Christa Seid, "Consumer sentiment evolves as the next "normal" approaches", McKinsey & Company (12 May 2020) <https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/a-global-view-of-how-consumer-behavior-is-changing-amid-covid-19> (accessed 18 May 2020); Cass R. Sunstein, *The Meaning of Masks*, FORTHCOMING JOURNAL OF BEHAVIORAL ECONOMICS FOR POLICY (2020) <https://ssrn.com/abstract=3571428>

particulars.[16] Innocuous as these provisions seemed when they were activated, there is growing disquiet over what happens to the data they collect, process and share/disseminate.[17]

Acknowledging these peremptory questions, the regulatory agenda that follows rests on several prevailing regulatory maxims, when it comes to personal data protection, and the use of AI and big data. In most jurisdictions, regional conventions and international instruments, there is recognition of the necessity to protect personal data, both in the interests of the data subject and for the integrity of the data itself.[18] While the limitations on personal data protection, and privacy regulation more generally are widely understood,[19] and there is often contention surrounding what is a challenge to personal data and privacy,[20] constitutional rights of privacy and administrative/legislative activity for the protection of personal data supports regulation in the case at hand.[21] Additionally, the technologies employed in the data accumulation around COVID containment, either qualify as AI, are AI-assisted, use big data or rely on internet-based communication pathways. This AI dimension places these control devices and frameworks squarely within corporate, national and international strategies which employ ethical principles governing the use of AI and big data. There is a groundswell of public opinion questioning the data safety of these technologies and asking for guarantees that the use of personal data will be limited to the exigencies of the health crisis.[22] Finally, the private contracts which consumers negotiate with mobile communication providers, and the privacy policies of social media platforms and private and public data collectors and

---

[16] "What is SafeEntry?", Safe Entry <https://support.safeentry.gov.sg/hc/en-us/articles/900000667463-What-is-SafeEntry-> (accessed 18 May 2020); "COVID-19: SafeEntry digital check-in system deployed to more than 16,000 venues", Channel News Asia (9 May 2020) <https://www.channelnewsasia.com/news/singapore/covid-19-safe-entry-digital-checkin-deployed-16000-venues-12717392> (accessed 18 May 2020)

[17] Even though Safe Entry has not been addressed from a data protection perspective in Singapore, experts around the world have raised their concerns about similar initiatives. Genevieve Bellarchive, We need mass surveillance to fight covid-19—but it doesn't have to be creepy, MIT Technology Review (12 April 2020) < https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/> (accessed 18 May 2020); 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)

[18] Graham Greenleaf, *Global Data Privacy Laws 2019: 132 National Laws & Many Bills,* 157 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, 14-18 (2019) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 >; Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, 106 GEORGETOWN LAW JOURNAL 115 (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066971>

[19] Graham Greenleaf, *Global Data Privacy Laws 2019: 132 National Laws & Many Bills,* 157 PRIVACY LAWS & BUSINESS INTERNATIONAL REPORT, 14-18 (2019) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593 >; Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy*, 106 GEORGETOWN LAW JOURNAL 115 (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066971>

[20] 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

[21] Constitutional legality, particularly when creating and enforcing rights of privacy, is a powerful, but not universally ascribed regulatory foundation.

[22] Mark Findlay, Jia Yuan Loke, Nydia Remolina, Benjamin Tham, *Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-crisis,* SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/02 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592283>

processors may run contrary to any of the data sharing practices that have emerged during the COVID-19 containment crisis.

It is important to note at this juncture that regulatory priorities may vary depending on political, economic and social context. For instance, in places where cultures of habitation are more communal, personal 'space' is limited, social hierarchies are intrusive, economic conditions exploitative, or styles of governance authoritarian, then privacy claims may be less well-enunciated and understood, or respected and actionable. Even so, there are fundamental and universal characteristics which attend on human dignity, humane society and inclusive governance that should be a core aspirational focus of personal data protection.

Moving from that commitment, it would be naïve to ignore the differential attitudes to the regulation of data protection region-to-region. Currently, in Europe, the UK and Australia there has been much debate surrounding the operation of smartphone tracing apps, with particular reference to voluntary versus compulsory usage, centralised versus individualised data storage, and private plus public information platform alliances.[23] This debate has raised protective options such as algorithm audits, data protection commissions, and independent recurrent evaluation.[24] Often these protection proposals are premised on pre-existing data management infrastructure, backed up by extensive enactments or protocols. Sophisticated debates about the enforcement of protective guarantees make sense in that context.[25] However, for the rest of the world, such as India, yet to legislate for general data protection, the nuances of such a regulatory discussion may be of little practical relevance when civil liberties and human dignity are at stake.

In those jurisdictions with identity card requirements for residents, then tracing and tracking may not appear initially as a much of major rights intrusion. In Singapore, the safe entry QR code tracing protocols could not function without there being a direct reporting link to the individual's NRIC (National Registration Identity Card)[26] However, in countries such as the United Kingdom and Australia where personal identity cards have been for decades vigorously opposed as human rights attacks by the state, this would be the foundation position from which in those jurisdictions, data protection initiatives around such a code process would progress.

Not wishing to raise regulatory options in the second half of this paper that either work from the lowest common denominator, or tend to further divide the world on the basis of privacy

[23] Jaewon Ryu and karen M. Murphy, Public-private partnerships for contact tracing can help stop Covid-19, STAT (24 April 2020) <https://www.statnews.com/2020/04/24/contact-tracing-public-private-partnerships-covid-19/>

[24] European Commission, E-Health Network, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States (15 April 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf>

[25] Monica Kuschewsky, DATA PROTECTION AND PRIVACY. JURISDICTIONAL COMPARISONS (Thomson Reuters, London) 2012; Megan Gray, *Understanding and Improving Privacy 'Audits' Under FTC Orders*, STANFORD CENTER FOR INTERNET & SOCIETY WORKING PAPER (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3165143>

[26] "What is SafeEntry?", Safe Entry <https://support.safeentry.gov.sg/hc/en-us/articles/900000667463-What-is-SafeEntry-> (accessed 18 May 2020); "COVID-19: SafeEntry digital check-in system deployed to more than 16,000 venues", Channel News Asia (9 May 2020) <https://www.channelnewsasia.com/news/singapore/covid-19-safe-entry-digital-checkin-deployed-16000-venues-12717392> (accessed 18 May 2020)

recognition and advanced data protection infrastructure, the analysis to follow highlights universal personal data usage challenge themes, such as anti-discrimination, that know few social, economic or political distinction. The regulatory preferences may be dependent on capacity and political will, but the need for regulatory action as we will propose against such universal challenges is unavoidable. While the private rights realms are often economically calibrated (based heavily around private property endorsement), [27] the United Nations Covenant on Civil and Political Rights offers basic and universal measures of human dignity that are non-derogable. We advance a universalist regulatory position and leave the specific nature of the regulatory technology preferred to policy makers mindful of their pre-existing regulatory infrastructure.

To draw these general observations to a close, the regulatory influence of ethical principles on the AI assisted technology and big data use that characterise the nature of COVID-19 surveillance strategies might be advanced as a broad regulatory umbrella for specific regulatory engagement, or even as a substitute for such specificity. It is not intended here to re-iterate the reservations associated with an ethics principle approach to the governance of AI and big data which is detailed in our recent research publication on the matter.[28] Power differentials internal to the AI ecosystem, market and client pressures and profitability demands militate against ethics as a sole effective regulator of AI and big data. In addition, the generality of the principles espoused in most ethical guidelines make them difficult to apply on a context-specific, or situationally relative basis. Therefore, regarding the regulatory approaches outlined to come, ethical aspirations form a strong normative morality which must pervade regulation's particular purposes and directions. The importance of human/individual dignity has already been mentioned. In what follows the significance of fairness, an anti-harm consciousness, and above all transparency and accountability will recur.

The case for regulation being complex but made out, it is now essential to give form and purpose to any proposed regulatory strategy discussed in Part 3. For present purposes there are several different structural approaches that present themselves:

- Highlight an essential regulatory obligation which binds together all the possible challenges posed by surveillance technologies and consequent data use - This *central theme approach* runs the risk of down-playing or bypassing other important themes.

- Follow a more conventional pattern and link regulatory techniques to individual data-use challenges - The difficulty with this is approach is that it tends to become repetitive and is too causally dependent.

- Group the challenges under 'liberty/integrity'; 'authority/legitimacy'; 'good governance/data justice' themes and form there consolidate regulatory responses - This approach seems formalist and may tend to predetermine regulatory selection

[27] Mark Findlay, *Laws Regulatory Relevance: Property, power and market economies* Edward Elgar, Cheltenham, (2017).

[28] Mark Findlay and Josephine Seah, *An Ecosystem Approach to Ethical AI and Data Use*, SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/03 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3597912>

- Reverse that approach by setting out a menu of likely and appropriate regulatory technologies and then group data challenges under these options - This approach has the advantage of identifying the regulatory sponsors (state/industry/civil society) more directly.

To make the choice and extrapolate the potentials of a regulatory strategy more focussed, accessible and relevant to an audience with different views on regulatory need the strategy is framed around three typologies of challenge to personal data – 'individual liberty/integrity'; 'authority/legitimacy and accountability'; and 'good governance and data justice'. In higher order the strategy intends not to exacerbate negative consequences already featuring and emerging from control approaches. There are three encompassing normative foundations for the regulatory exercise.

1. *Lessen and avoid discrimination* – there are instances in the operation of these technologies, their understanding, coverage and data-use consequences of discrimination against the aged, infirmed, ill-informed, anxious, polarised, poor and those without adequate capacity to comply. Regulation cannot cure all structural inequalities prevailing around surveillance technologies and data use, but it can be mindful of these, and as with bias, prevent both the data usage and its regulation fuelling prevailing or emerging discrimination.

2. *Recognise and comply with established principles of ethical AI, big data use, and principled design* - Paramount among these principles for our purposes are
    - Human dignity and solidarity when directed to individual liberty/integrity
    - Transparency and explainability when directed to authority/legitimacy and accountability
    - Fairness and harm avoidance when directed to good governance and data justice

3. *Promote citizen inclusion* – while protective health and safety controls tend to be paternalistic, they will no matter how well intentioned, for the most supportive up-take, require the broadest engagement across communities, and should offer inclusive, simple and satisfactory opportunities for conflict resolution. It is not enough for the state or the big private sector data repositories to ask for compliance and unquestioned trust when many of the risks associated with surveillance and data usage are not candidly revealed and openly negotiated.

We have decided not to focus the regulatory direction first on surveillance technologies or data sharing as the organisational focus. The reason is that by taking such an approach the proposed strategy exposes itself to reservations such as 'What if these technologies and data sharing practices are happening anyway or in other contexts? Do we want to regulate everything?' Giving workable parameters to the proposed regulatory exercise, what follows is only interested in confronting tech/data applications as the *devices creating challenges*, and not the challenges in themselves. Through regulation it is personal data use challenges, not technologies themselves, that will be addressed by regulatory tools. Many pre-existing surveillance technologies/data use practices, for our purposes, have become intrusive

because of the pandemic justification. With the crisis purpose justified, empirically audited and externally overseen[29] ancillary data usage is our limited field of interest.

The missing question after 'what, where, when and why', is who. A common failing of regulatory overviews is to stipulate responsibility without specific attribution. Of course, in some instances, the nature of the regulatory technology will indicate its authority. Command and control approaches require state sponsorship. Self-regulation invites more diverse stakeholder participation. However, there is a need to identify conundrums that attach to attribution and distribution of responsibility:

- This is a global pandemic, but outside what some say is the World Health Organisation's problematic co-ordinated response across its members, sporadic acts of generosity with medical services and equipment, and some trans-national cooperation in vaccine research, control strategies have almost all emerged within nation-state priorities. There has been little in the way of international cooperation which was a common feature of pandemics in the past. This reluctance to engage cannot be a consequence of insufficient international infra-structure, or technological incapacities for sharing and integration. The more accurate explanation may lie in the *ad hoc* manner in which many states have managed a health threat that seems to have caught them off-guard and ill-prepared. More recently, this state self-interest has degenerated into the scapegoating of other nations in efforts to deflect political pressure at home.[30] Hopefully, the joint scientific endeavours at finding a vaccine and communication of treatment research across borders will see international control responses survive political expedience. If this is so then an opportunity exists to craft global regulatory responsibilities.[31]

- Regulatory attribution is often most efficient when it is a collective endeavour. Because of their responsibilities for the provision of health care at large state agencies obviously assume an important role, or the more so when compulsory powers or enforcement potentials are required. Public and private sector providers and

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

[30] Michael H. Fuchs, "The US-China coronavirus blame game is undermining diplomacy", *The Guardian* (31 March 2020) https://www.theguardian.com/commentisfree/2020/mar/31/us-china-coronavirus-diplomacy>; "China emerges as coronavirus scapegoat in US election campaign", *AlJazeera* (18 April 2020) https://www.aljazeera.com/news/2020/04/china-emerges-coronavirus-scapegoat-election-campaign-200417155934233.html (accessed 20 May 2020)

[31] For instance, the Organisation for Economic Co-operation and Development (OECD) has stated that the COVID-19 emergency makes the need for trusted, evidence-based, internationally coordinated and well-enforced regulation particularly acute. While "emergency" regulations may be adopted and non-critical administrative barriers lifted, Governments still need to uphold the well tested principles of good regulatory practices. A wide array of international regulatory co-operation approaches can be used to align government responses, including international evidence gathering and sharing to aid in the design of emergency rules, aligning regulations or using mutual recognition to expedite administrative processes and facilitate the trade of essential products, such as protective equipment, for example. International organisations provide essential platforms to promote such co-operation. Organisation for Economic Co-operation and Development, "Regulatory quality and COVID-19: Managing the risks and supporting the recovery" <http://www.oecd.org/coronavirus/policy-responses/regulatory-quality-and-covid-19-managing-the-risks-and-supporting-the-recovery-3f752e60/> (accessed 20 May 2020)

administrators of surveillance technology transmit common due-diligence and best practice obligations as a result of the benefits they gain in any market sense. Civil society carries reporting and community oversight functions, provided they are given sufficient information to enable potent participation in the regulatory exercise. Social and conventional media represent an important public education function and a facility for accountable debate provided reporting does not degenerate into misinformation or propaganda for any particular dogma.[32]

- Where personal data is being shared by different private communication platforms and between public and private providers private law through service contracts is likely to create regulatory obligations on these entities for the benefit of their customers.

- Public law in the form of data protection instruments may vest authority in independent agencies to perform regulatory functions. Independent regulation institutions and processes are particularly prominent when the purpose is to generate trust in the data management regime.

- Ultimately, and in a simple configuration when addressing regulatory attribution the paper progresses with this rule of thumb; *depending on who it is that advocates and promotes and administers control technologies automatically producing personal data that could be misused, or to the harm of the data subject, then the responsibility to build in regulatory strategies to avoid harm and misuse rests first with them.*

PART 2. Ethical Challenges

In a recent work the Centre for AI and Data Governance of the Singapore Management University (CAIDG) has identified a series of potential challenges to personal data and data subjects arising out of COVID control-applied surveillance, tracking, quarantine and movement technologies and processes.[33] Based on this previous research, this section summarizes the challenging consequences for mass data use beyond any determined limits of crisis containment. The control strategies producing personal data challenges are risk/benefit in nature and involve contestation between political/economic and health interests. 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. Even so, if regulatory

[32] Gordon Pennycook, Jonathon McPhetres, Yunhao Zhang and David G. Rand, *Fighting COVID-19 misinformation on social media: Experimental evidence for a scalable accuracy nudge intervention*, MIT INITIATIVE ON THE DIGITAL ECONOMY WORKING PAPER (2020) <http://ide.mit.edu/sites/default/files/publications/Covid-19%20fake%20news%20ms_psyarxiv.pdf>; Jayaseelan R, Brindha D, Kades Waran, *Social Media Reigned by Information or Misinformation About COVID-19: A Phenomenological Study,* SOCIAL SCIENCES & HUMANITIES OPEN D-20-00130 (2020), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3596058>

[33] Mark Findlay, Jia Yuan Loke, Nydia Remolina, Benjamin Tham, *Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-crisis,* SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/02 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592283>

intervention is operationalised early (as we advocate in the final part) then personal data protection will be an objective in the control initiatives as much as risk/harm prevention.

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,[34] or to play a part in containing the virus, counter-narratives have emerged which rehearse reservations about the consequences of such mass data sharing.[35] 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.

As with Part 3, the ordering of topics will follow the normative foundations for the regulatory endeavour: to reduce discrimination; to comply with ethical principles for AI and data use; and to promote citizen inclusion through best practice and good governance standards.

Discrimination

In this pandemic, we observe discrimination along the lines of income, occupation, socioeconomic status, ethnicity, race, nationality, gender, housing situation, and more.[36] African people in China are perceived as more infectious.[37] Low-income groups are more likely to have jobs that must be performed on-site. Women and LGBTI groups may find working from home more challenging.[38] As is the case with many, if not all, social issues, these patterns of discrimination *intersect* and overlap. A person with a low income is more likely to live in substandard housing, have a job that cannot be performed remotely, and so on.

Discrimination can arise in two pandemic-related sites. First, discrimination arising from the pandemic harm (vulnerability and risk), and second, discrimination exacerbated through the data-harvesting and data usage control strategies in the crisis period. Flowing from these, for a regulatory mission with anti-discrimination as a concern for both regulatory intervention and for its outcomes, (beyond structural repositioning of poverty and disadvantage which we have to take as a given) regulatory interventions can and should minimise both forms of discrimination

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

[35] 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)

[36] There is, of course, a large body of literature investigating and unpacking the various terms. In this project we are unable to define each term and do justice to its nuances.

[37] Human Rights Watch, "China: Covid-19 Discrimination Against Africans"(5 May 2020) <https://www.hrw.org/news/2020/05/05/china-covid-19-discrimination-against-africans> (accessed 20 May 2020)

[38] Morfi Jimenez, "COVID-19: Rights Experts Highlight LGBTI Discrimination, Antisemitism", *UN News* (17 April 2020) <https://news.un.org/en/story/2020/04/1062042> (accessed 20 May 2020)

It has been argued that in the sense of data applications, discrimination can be viewed as mis-categorisation, seeing different individuals and groups in society as the same and overlooking essential differences. Responding to COVID-19 requires a lot of categorisation. Emergency events demand immediate planning and response which is filtered by categories of need and resilience. There may limited time for fine-tuning and getting every detail right. However, as is revealed by the necessity to mass quarantine whole sub-sets of populations, some of the most vulnerable groups have not registered soon enough in the minds of controllers as presenting unique differences.[39]

Governments are not the only actors who need to respond quickly: companies and universities scramble to make arrangements for their workforce and students, communities have to adjust to new ways of living. Authorities and societies place individuals into categories in order to measure, monitor, manage, and make sense of the crisis. In doing so, profound social characteristics are too often universalised. The following are general patterns of discrimination through mis-categorisation:

1. *Authorities and societies employ new categories that are not used in normal times. We treat people in different categories differently***.** This is not first and foremost discrimination but may enable it. For example, taking precautions to manage people in the "infectious" category seems fair. But in some cases, we observe needless bullying and ostracism of the sick, their families, and health workers.[40]
2. *Sometimes, we miscategorise similar people***.** For example, in many countries Chinese people, Africans or Hispanics are more likely to get categorised as "infectious".[41] This mis-categorisation--combined with the fact that infectious people are treated differently--results in discrimination.
3. *Authorities and societies fit dissimilar people into the same category. Some people fit more easily into their assigned category than others***.** For example, many students have to study from home, but low-income students find it especially challenging, not just for lack of private space but because their subsistence may be jeopardised by loss of

[39] Kolitha Wickramage, Lawrence O. Gostin, Eric Friedman, Phusit Prakongsai, Rapeepong Suphanchaimat, Charles Hui, Patrick Duigan, Eliana Barragan, and David R. Harper, *Where Are the Migrants in Pandemic Influenza Preparedness Plans?,* HEALTH AND HUMAN RIGHTS JOURNAL V. 20(1) (2018) <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6039731/>; The International Committee of the Red Cross (ICRC), *Note on the protection of migrants in the face of the covid-19 pandemic* (2020) <https://www.icrc.org/en/download/file/117261/public_note_on_the_protection_of_migrants_in_the_face_of_the_covid-19_pandemic_08.04.2020.pdf> (accessed 20 May 2020)

[40] The Associated Press, "In Japan, Pandemic Brings Outbreaks of Bullying, Ostracism", *The New York Times* (9 May 2020) <https://www.nytimes.com/aponline/2020/05/09/world/asia/ap-asvirus-outbreak-japan-corona-discrimination.html>

[41] Sherita Hill Golden, Coronavirus in African Americans and Other People of Color, Johns Hopkins Medicine website <https://www.hopkinsmedicine.org/health/conditions-and-diseases/coronavirus/covid19-racial-disparities> (accessed 20 May 2020); Stephen Chen, "Covid-19 hits African-Americans hardest in 'potential catastrophe of inequality', US study finds", *South China Morning Post (*1 May 2020) <https://www.scmp.com/news/china/science/article/3082470/covid-19-hits-african-americans-hardest-potential-catastrophe> (accessed 20 May 2020)

> casual employment.[42] Regularly, explicit differences that were previously less visible or less or an issue are focused on with unfair consequences. For example, the difference between people who can work from home and people who must work on-site is illuminated when we lump everybody into the social distancing imperative, and as such expect everyone is equally protected.

Over all, the line between new and pre-existing forms of discrimination is not crisp. However, it can be made much more operationally distinct if data-harvesters and users employ documented knowledge concerning *vulnerability* (to infection, to non-compliance with control strategies, and to discriminatory outcomes from data application), then 'difference' can become both a potent control tool and a significant regulatory backdrop.

It is important to remember that the consequences of failure to discriminate in safety measures, and then mass discrimination in control responses are not to be dismissed as high order concerns incompatible with crisis conditions. In situations where mass quarantining has led to disease incubation resulting from failing to plan for vulnerability, a range of new regulatory obligations arise which relate to ramping up testing and medical services for the discriminated populations involved.[43]

Individual dignity

Human dignity is a leading principle in public health ethics.[44] Health data is considered sensitive data in most jurisdictions meaning that data processors in this context regularly and routinely are subject to particularly strict rules.[45] Since the coronavirus outbreak at the beginning of 2020, a number of countries have documented bias, racism, xenophobia, and discrimination against people of Asia, from Asia in North world settings, and more recently against foreigners in Asian countries like China.[46]

---

[42] Venessa Lee and Stephanie Yeo, "How Home-Based Learning Shows up Inequality in Singapore - a Look at Three Homes"," *The Straits Times* (18 April 2020) <https://www.straitstimes.com/lifestyle/how-home-based-learning-hbl-shows-up-inequality-in-singapore-a-look-at-three-homes> (accessed 20 May 2020)

[43] Linette Lai, "Singapore has been ramping up testing for coronavirus to help curb spread", *The Straits Times* (28 April 2020) <https://www.straitstimes.com/singapore/spore-has-been-ramping-up-testing-for-virus-to-help-curb-spread> (accessed 20 May 2020); Yuen Sin, "Covid-19 outbreak brings migrant workers from margin to centre of Singapore's attention", *The Straits Times* (30 April 2020) <https://www.straitstimes.com/opinion/migrant-workers-from-margin-to-centre-of-spores-attention> (accessed 20 May 2020); Hillary Leung, "Singapore Was a Coronavirus Success Story—Until an Outbreak Showed How Vulnerable Workers Can Fall Through the Cracks", *Time* (29 April 2020) <https://time.com/5825261/singapore-coronavirus-migrant-workers-inequality/> (accessed 20 May 2020)

[44] 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

[45] 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.

[46] 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.

Discrimination based on presumed spread of the virus may have serious consequences for human dignity.[47] Respect for the integrity of one's personal data is indeed an integral part of human dignity. Unfortunately, the value of life when it comes to human subject testing and the availability of treatment and vaccine services during and post pandemic set a climate where human dignity is differentially valued.[48] In philosophical anthropology, there are different views about human dignity, and hence different ways of defending personal integrity in terms of privacy or otherwise.[49] 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 apprehension for human dignity. Aligned with this concern is the reality that the integrity of personal data can have direct influence, positive and negative on human dignity and its representation.

Individual dignity in its practical manifestations is hard to extract from social identity and economic sustainability. Presently, 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,[50] and based on immunity status, issue an "immunity passports".[51] This approach should not be confused with a pre-emptive tracing initiative, and 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.[52] China is presently implementing a less

---

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)

[47] Ryan Thoreson, "Covid-19 Backlash Targets LGBT People in South Korea. Government Should Act to Prevent Discrimination", *Human Rights Watch* (13 May 2020) <https://www.hrw.org/news/2020/05/13/covid-19-backlash-targets-lgbt-people-south-korea> (accessed 20 May 2020)

[48] Mark Findlay, *Contemporary Challenges in Regulating Global Crises,* Palgrave Macmillan, (2013), chap 5.

[49] 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

[50] 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.

[51] 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)

[52] 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)

hard-edged scheme where individuals seeking to travel in the country must obtain and display a health certification certificate, on their mobile devices. [53]

Transparency

Ethical pre-requisites for the use of AI-assisted technologies and big data resonate with interests in solidarity, dignity and social responsibility.[54] It becomes nigh on impossible to empower individuals to assert dignity and solidarity if they remain ignorant of personal data production and its varied applications. 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.[55] 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 and community compliance and trust, is the same confidence transferred to private companies turning over their location data to governmental agencies unless the data-subject 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, which harvested personal data is tracing and logging.

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.[56] Such transparency is even more important in countries like 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

[53] 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." See "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)

[54] 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)

[55] 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)

[56] 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)

individual liberties are mandated constitutionally.[57] Some companies already share aggregate data, but it would be new for Google and Facebook to openly mine user movements on this scale for government surveillance purposes. The data collected would show patterns of user movements. It would need to be cross-referenced with data on testing and diagnoses to reveal how individual and group 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.[58]

Transparency is at the heart of regulatory accountability. It is impossible to operate an inclusive accountability environment where personal data is concerned without data transparency. But in this demand lurks counter-concerns for privacy compromise through transparency. Space does not allow for a fuller discussion of the tensions between data protection and wider information access when control/safety imperatives are involved, and consequent data-subject notification is advocated. Sufficient for the regulatory purpose is to recognise these tensions and to ensure anonymised information looping which keeps data subjects informed about pathways of usage.

Avoiding Biases

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, requires likely identification and corrective action. There is nothing new in the challenge of data bias particularly where identification technology draws discriminatory conclusions on race and gender. In a pandemic bias 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, excessive or ineffective 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.[59] Against this experience, it is necessary to ensure that any automated data systems

[57] 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)

[58] 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)

[59] 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

used to contain COVID-19 do not erroneously identify members of specific demographic groups as particularly susceptible to infection.[60] 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.[61]

Computer scientists have shown that facial recognition has greater difficulty differentiating between men and women the darker their skin tone. A woman with dark skin is much more likely to be mistaken for a man.[62] This limitation could lead to people of colour being wrongly identified as potential carriers.

Bias eradication is not only a technological issue. Policy makers and their communities operate in climates of bias such as racism which are not dependent on technological manifestation. Technology comes in and has the massive potential of bias exacerbation, and even legitimation through algorithmic processing.

Explainability

Comprehension of the legitimate purposes for personal data-harvesting and data usage in crisis contexts is also reliant on trust in the information provided and the intentions of those who provide it. Trust will be produced through transparent explanations of benefit and risk, particularly to the vulnerable and disenfranchised. 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 domestic/employment relationships or travel), in some jurisdictions[63] the data subject should have the opportunity

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)

[60] 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)

[61] 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)

[62] 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

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

for timely and fair challenging of these conclusions and limits.[64] Moreover, explainability is a guiding principle within most if not all the ethical data use guidelines that companies and governments have published.[65] 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.

General comprehension of emergency measures and their impact act as a bridge between transparency and accountability. Explainability is ultimately in the interests of private and public engagement and the appreciation of balanced policy planning

Public interest versus individual rights

To introduce this challenge, it would appear that the issues are essentially dichotomous. As part 3 will re-iterate, if public interest motivations are prosecuted with a conscious appreciation of private rights then proportional compatibility is achievable. Unfortunately, however, the political discourse surrounding control regimes is couched in terms of sacrificing individua rights for communal benefit. So, stay-home orders and social distancing are seen inevitably as compromising liberties of association and movement. This is not how part 3 will see these coefficients. Short term movement restrictions are only intended to make greater socialisation a medium-term option. In this consideration both the public and private interests are collapsed and any interference with private liberties is a temporal question.

These surveillance programmes are based on reasons related to public interest in controlling the spread of the COVID-19 pandemic. 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.[66] 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

---

[64] 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)

[65] 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)

[66] 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)

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 contexts.[67] Some forms of authority, for instance, use exemptions in data protection laws to share data.[68] Most of these measures claim to be temporary, necessary, and proportionate. However, largely they have not addressed ethical issues so far.[69]

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.[70] Personal physical safety threats prompt a willingness to compromise individual protections and liberties. These threats and their associated community confrontation also introduce notions of perverse citizenship, where it is good to comply, risking discrimination and social rejection if one does not. This subliminal deterrence acts as 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 apps could be used to extend emergency measures beyond the crisis, an outcome that many 'good citizens' would oppose.[71]

This 'shaming' strategy based on 'fear if you do – and fear if you don't' 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

---

[67] For instance, the Infectious Diseases Act (IDA), which was enacted by Parliament in 1976 and came into force on 1 Aug 1977, is the principal piece of legislation that deals with the prevention and control of infectious diseases in Singapore. Infectious Diseases Act, Singapore Statutes Online website <https://sso.agc.gov.sg/Act/IDA1976> (accessed 20 May 2020)

[68] 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 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)

[69] Mark Findlay, Jia Yuan Loke, Nydia Remolina, Benjamin Tham, *Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-crisis,* SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/02 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592283>

[70] "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)

[71] Lorenzo Franceschi-Bicchierai, "Am I a Jerk for Refusing to Use a Coronavirus Contact Tracing App?", *Vice* (13 May 2020) <https://www.vice.com/en_us/article/4ayywp/refusing-to-use-coronavirus-contact-tracing-app> (accessed 20 May 2020)

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[72] can make salient the public gains from mass adoption, thereby appealing to social norms and peer pressure in further encouraging app adoption.[73] Texts could also make people aware of the extent to which others in their community, or neighbouring communities, have downloaded the app, associated research suggesting that unfavourable social comparisons would motivate app adoption.[74]

National border closures have become the norm. In particular 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.

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

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

[73] 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 Australia 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 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)

[74] 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>

people who may have been exposed to the virus - and other minimally invasive alternatives are not suitable —e.g., using anonymised mobile positioning data.[75]

Nonetheless, aggregate, anonymised location data is already made available to researchers by Google, Facebook, Uber, and cell phone companies, often monetised in clandestine secondary market frames.[76] 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.[77]

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.[78] It is important to avoid the creating of a compulsory or convenient tool that enables large-scale data collection on the population beyond the defined limits of crisis health safety purposes. An example is the application of Qr codes for safe-entry and exit tracing. It would seem that associated personal data is innocuous enough. But, what if governments implemented such entry and exit tracing not only to monitor individual movement but to permit or prevent certain classes of citizen from obtaining access to certain facilities, based on other shared data such as travel history, ethnicity, religious persuasion, financial standing and other discriminatory demographics (all which may be available through the link to the national identity card data bases)? Along these lines, more than 300 academics warned the National Health Services in England about solutions that allow reconstructing invasive information about the population around movement and aligned health status. Those potentials, it was argued, should be rejected from the design.[79]

---

[75] 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)

[76] Kirsten E. Martin, *Ethical Issues in the Big Data Industry,* ASSOCIATION FOR INFORMATION SYSTEMS MIS QUARTERLY EXECUTIVE 14:2 (2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2598956>

[77] 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)

[78] 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).

[79] 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)

Expiration[80]

There is a key difference as we see it between transparency and explainability. Data subjects may know about and approve the limited use of their personal data during crisis times, but not continue with compliance if the discriminatory or continuing invasive possibilities are maintained when the emergency is over but the data lives on. 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. If, for instance, some of the demographic simply referred to as 'the majority of infections' and designated by their quarantined location, may be happy existing as a percentage, but not being negatively identified after the infection has been treated as someone once having had the virus. This stigma ongoing could bounce up in personal health, employment and travel records every time the subject wished to work, seek a medical clearance or look to extend their immigration permits.

It might be considered not in their wider social engineering interests for some governments to qualify these surveillance methods after crisis justifications have diminished, by ceasing data-harvesting and destroying data storage. 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 obliged to roll back any invasive programs created in the name of public health after crisis has been contained.[81] 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.[82] 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

[80] 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.

[81] 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)

[82] 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

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.

Aligned with data rehabilitation/expiration regulations is the concern for firewalling databases. In jurisdictions where criminal record information is given a shelf-life after which expiration is automatic except the justification that making such data forever active defeats some many other important considerations in returning offenders to productive social contributors without carrying the burden of outmoded stigma.

PART 3. Regulatory strategies and Policy Recommendations

An informed reflection on 'crisis' mass data usage in transitional and post COVID-19 eras necessitates a prior 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. Reflecting on Part 2, it was important to elaborate these data-harvesting and use challenges, prior to discussing the significance of their regulation so that any image of a clear and stable demarcation between crisis and post-crisis lifestyles is disabused. The proposals to follow do not depend on the extinguishing of any crisis justification for such data-harvesting and use. Instead, the regulatory invocations are seen as necessarily running during the period of crisis activation, and then being employed in the decommissioning of these harvesting and usage regimes, and the remission of the data accumulated as the crisis justifications no longer prevail.

General regulatory fundamentals

Accepting that regulation starts now there will be constant and ongoing instances of where deliberations on access against protection, and extraordinary use compared with institutionalised conventional safeguards will require evaluation around use-case necessities, as the crisis winds down. Additionally, COVID-19 will not be the only global pandemic of this type to confront human futures and there will need to be prevailing appraisal of reasonable conditions to qualify regulatory universals. These observations mean that any realistic regulatory framework should include an arbitration/conciliation facility that will responsibly weigh competing externalities and adjust regulatory requirements to reflect safety/risk imperatives which may never fully extinguish.

With that concession presented, the challenges posed by any ongoing application of intrusive data-harvesting technologies created or augmented during crisis conditions, and lax data sharing limitations enabling mass data application for similar control justifications pose very grave ramifications for personal data integrity and the embedding of unrepresentative and disempowering surveillance societies.[83] Therefore, vigorous and powerful regulatory infrastructure and process need implementation as matters of urgency.

[83] 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-

We have already indicated that the regulatory options set out in this part are designed to be thematic and not proscriptive. That intention recognises that there will be different regulatory capacities and styles jurisdiction to jurisdiction, region to region, and across different regulatory challenges. Even so it is necessary, for the sake of consistent regulatory attainment to present three particular technologies/institutions/processes, that reflect our concerns about enforceability, engagement and citizen empowerment. In brief summary it is proposed that these regulatory cornerstones should be created:

A. COVID Personal Data Commissioner[84] (CPDC) – this agency would have carriage for researching potential personal data challenges transitioning out of the health crisis. It would have a public education consultation and complaints function. In addition, it would act as a personal data access arbitrator, to determine applications for access against data protection protocols. Finally, it would house a licensing function for data technologies, repositories and expiration requirements. Preferably the Commissioner would be an independent agency with legislative authority, reporting to a board of public and private sector data-harvesters and users, and representatives of other data protection instrumentalities, and civil society.[85]

B. *Enforced Self-regulation Units* (ESU) - tasked with the responsible operation and eventual decommissioning of surveillance technologies, and their data repositories, on a technology-specific focus. The CPDC would act as the independent agency in the enforced self-regulatory model. These units would determine compliance guidelines in consultation with the CPDC, public and private stakeholders, and civil society.

C. *Civil Society Empowerment Initiatives* (CSEI) – during the COVID-19 crisis many countries and communities have seen the emergence of organised and informal community endeavours designed to assist in and propagate the risk/safety control message, As a counterbalance to the negative impact strenuous data protection regulation may have on current and future pandemic control strategies, now and

public-health-crisis> (accessed 2 April 2020); Mark Findlay, Jia Yuan Loke, Nydia Remolina, Benjamin Tham, *Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-emptive Tracing Post-crisis,* SMU CENTRE FOR AI & DATA GOVERNANCE RESEARCH PAPER NO. 2020/02 (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3592283>

[84] There has been some debate in regulatory circles as to whether a purpose-designed data protection administration should be created in the COVID-19 climate, or if passing over responsibilities to existing data protection agencies would be sufficient. For the present in the UK the Information Commission is addressing COVID data concerns. However, we believe that the new technologies and mass data sharing in the COVID control agenda are so unique and present such context-specific personal data challenges that a new agency needs the brief. Many pre-existing data protection agencies have limitations of coverage (such as not looking into public sector data use) as to make them substantively incapable of performing the required regulatory oversight. If each new global pandemic necessitates its own data protection infra structure will similarly depend on whether the tech and usage dimensions of the response at the time are markedly different from the COVID experience.

[85] Such a multi-functional authority that uses licensing as an enforcement parameter resembles formats that have been advanced internationally for independent financial regulation. The licensing capacity is also crucial in Braithwaite's enforced self-regulation model.

ongoing, this volunteer power-base needs to be enhanced and institutionalised to assist in ensuring the safety conditions of the 'new normal' as the virus crisis transits from an immediate threat to a feature of health care horizons.

There may be two initial reservations raised against the proposals above. Cost and complexity are one. The other is an overreliance on the heavy hand of the state. Responding to the cost and complexity concern which no doubt locates in a), while we prefer the establishment of a purpose-designed authority there is nothing arguing against its location within a permanent and more generalised data-protection administration. An approach like this would protect against costly duplication and unnecessary overlap and offer economies of scale in administrative capacity and operational infrastructure. In addition, representing tightly confined duties and responsibilities the legislative super-structure for the CCPC would be simple and uncontentious.

As for an over-reliance on state sponsorship, b) and c) are self-regulation technologies in primary operation. Further, each of these three proposed technologies appear beneath the earlier mentioned regulatory attribution of first resort – those who are promoting the technologies for tracking, tracing, surveillance, quarantine containment and safe entry have initial responsibility to ensure that automatically produced personal data are sufficiently protected within the operation of the technology and consequent data use. As is the common understanding in enforced self-regulation models, most data use challenges will be met at the lowest level of the regulatory pyramid and this would be no exception in our view, assuming the promoters of the control; technology are acting in the public interest at large.

Why would state and private sector data-harvesters and sharing data platforms want to give up windfall data access gains that the virus crisis had offered ongoing. We speculate two reasons:

a) *Generation of long-term trust*. Science warns that this will not be the last global health pandemic states and regions should plan for. A general criticism or the responses to COVID-19 has been the lack of preparedness despite years of serious forewarning.[86] Associated with this failing was a general public insufficiently equipped, informed and ready for the necessary intrusions that surveillance and movement regulation would entail. Put these two factors together and when contact tracing apps were mooted swathes of society were neither willing to trust the technology or the promoter's assurances.[87] To avoid any tragic repeat of this resistance in future crises, and to learn from mistakes around the control strategy communication, if communities could be

[86] University of Wyoming, "Lack of COVID-19 preparedness in line with previous findings, economists find", *ScienceDaily* (14 May 2020) <www.sciencedaily.com/releases/2020/05/200514115734.htm> (accessed 20 May 2020); Alexandra Brzozowski, "COVID-19 pandemic raises questions on preparedness for biological threats", Euractive (30 March 2020) <https://www.euractiv.com/section/defence-and-security/news/covid-19-pandemic-raises-questions-on-preparedness-for-biological-threats/> (accessed 20 May 2020)

[87] Kate Cox, "Half of Americans won't trust contact-tracing apps, new poll finds", *Ars Technica* (30 April 2020) <https://arstechnica.com/tech-policy/2020/04/half-of-americans-wont-trust-contact-tracing-apps-new-poll-finds/> (accessed 20 May 2020); Carlos Cantú, Gong Cheng, Sebastian Doerr, Jon Frost and Leonardo Gambacorta, "On health and privacy: technology to combat the pandemic", *BIS Bulletin No 17* (19 May 2020) <https://www.bis.org/publ/bisbull17.pdf> (accessed 20 May 2020)

reassured by the responsible way key data players cooperated in the protection of personal data with the virus in transit, then the benefits are obvious for those responsible for health risk/safety administration, and considerable.

b) *Best-practice reputation*. The differential infection rates, horrifyingly exponential death tolls and contention over sourcing and spread have left some political (and scientific) reputations in tatters. These negative repercussions for national and regional standings will not be cured by financial bailouts or international enquiries alone. How countries come out the other side in terms of personal data protection and rejecting the temptations of a greater surveillance governance will offer hard proof of responsible regulatory commitment, ethical ascription, and a desire to show the world that universal rights and safeguards do not have to join the scale of human lives lost as the critical measure of control competence.

Challenges associated with regulating for individual liberty/integrity

Discrimination

The fight against COVID-19 exposed and exacerbated certain types of discrimination. Interventions that appear neutral on their face may license or facilitate racial bias, without care and attention. Thus far, no data protection efforts have focused the public health response on the specific vulnerabilities of certain populations (e.g. migrant workers, the incarcerated, the aged). Moreover, the outbreak has provoked social stigma and discriminatory behaviours against people of certain ethnic backgrounds as well as anyone perceived to have been in contact with the virus. This 'mark of Cain' atmosphere means that personal data about virus exposure is particularly risky for vulnerable and discriminated sectors of the community, and as such should receive precise protective focus.

In order to avoid discrimination in terms of personal data use and harmful conclusions drawn, governments can implement several measures. First, it is important to reduce asymmetries of information. People are more susceptible to biases and stereotypes when they lack accurate information. Clear, concise and culturally appropriate communication — in multiple forms and in multiple languages — is needed to reach broad segments of the population, with particular focus on marginalized communities. This approach can be taken up at a civil society engagement level where prevailing community-based bias is easier to identify.

Additionally, it is relevant to portray different ethnic groups, different age demographics and different levels of physical ability in public information materials about the virus and the emphasises the special need to protect the vulnerable. This approach has been adopted in certain situations when advertising degrees of social distancing. Images of diverse communities working together to reduce risk can powerfully communicate messages of solidarity and shared commitments to health and well-being. However, racial and gender tokenism particularly in the portrayal of health-care workers can have negative impacts and needs to be guarded against.

Finally, media reports which focus on individual behaviour and infected individuals' "responsibility" for having and spreading the virus can stigmatize these individuals and the groups from which they originate. News consumers should insist on responsible media reports that emphasize prevention practices, and individualised symptoms to look out for and when to seek care rather than stigmatizing of certain communities. Citizen awareness and professional news oversight bodies have a role to play

Principles to tackle possible discriminatory practices related to the fight against COVID-19 and the personal data uses should be included in the legal frameworks that regulated the infectious deceases control strategies. By so doing, anti-discrimination measures would not apply to the COVID-19 emergency alone, but also to any other form of data use in all infectious decease environments.

Quarantining control measures, usually imposed on otherwise virus vulnerable or discriminated populations such as migrant workers, confined aged care patients, prisoners and the military, can have a disease incubating effect. The consequent impact on how victim personal data is harvested, interpreted and maintained can complicate discrimination ongoing. The necessity for mass screening, ramped up medical services, humane isolation and progressive re-integration protocols are the responsibility of the quarantining authority as it operates its containment endeavours. At the same time, this authority must have in place personal data protection conventions for the manner in which aggravated infection has disadvantaged particular vulnerable sectors. These conventions should be drafted in consultation with the independent data protection agency. As mentioned above, if personal data produced in the circumstances of mass incubation is then transferred to other databases and subjects are harmed as a result, compensation opportunities need to be administered by an independent data protection agency, perhaps through a public complaints initiation and regular data-use monitoring.

Established anti-discrimination regulators and their legislative powers should not be diminished in their reach during pandemic emergency conditions.

Grass Roots Transparency and Accountability

The reasons behind any limitation of individual liberties and integrity should be publicly enunciated by those promoting the data-harvesting technology with this potential. Information regarding the positive and negative impacts on safety and identity should be clearly and candidly canvassed in forms and formats that are accessible and understandable to all communities that the technologies will cover (If the CPDC is adopted with licensing powers this information/communication obligation would be a condition of the license). As the scale and severity of the COVID-19 pandemic rose to the level of a global public health threat[88] justifying restrictions on certain rights,[89] then causal relations between threat,

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

[89] 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

control policy and intended outcomes must require informed and routine monitoring by civil society effected from intrusive technologies. Civil society can only perform a potent monitoring function if it is provided with up-to-date information, and constant information looping, that details the operation of data-harvesting. **Civil society monitoring** should be assisted by the regular review of operational objectives for the technology against rights and liberties measures, carried out by the technology promoters (Again, if the CDPC is adopted public awareness can also be facilitated within its mandate). 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 diseases."[90] 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. For these 'rights' to have localised meaning, technology promoters must translate principles into practice through a 'use-case approach' to control benefits and liberty/integrity intrusions (If ESU's are adopted and activated they would take on this regulatory responsibility). A useful way to embed this 'awareness' regulatory atmosphere is through recurrent and structured community consultations and conversations.[91]

Anxiety Reduction

Social and conventional media provide both positive and negative influences over community anxieties associated with the pandemic and its control. Depending on the emphasis, economic or scientific, reporting of virus control can condemn or extol the same strategies. Social distancing is a necessary measure to keep us safe or an authoritarian over-reaction that will ruin the economy. Guarding against anxiety-inducing media influence is much more than vigilance against fake news or pernicious reporting. Major news platform providers (social and conventional) in an atmosphere of anxiety and dangerous polarisation have a duty to provide balanced reporting. Unfortunately, in the COVID-19 outbreak they have patently

---

Globe", *The New York Times* (15 April 2020) <https://www.nytimes.com/article/coronavirus-travel-restrictions.html> (accessed 7 April 2020)

[90] 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. <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx> (accessed 20 May 2020)

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)

[91] European Commission, E-Health Network, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States (15 April 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf>

failed to maintain even unbiased news coverage. This expectation is difficult to achieve when certain influential politicians in particular dispute science and prefer misguided populism to evidence-based policy.[92]

The paternalist state can suggest it will protect us from the extremities and excess of AI and big data. As such, data protection laws become preventive, and individuals are nominated within their reach as vulnerable subjects who see risk in so many third-party applications of personal information which their profligate sharing has enabled, in turn, demanding state regulatory protection. Anxiety, distrust, and fear are institutionalized in this order, and it is a contemporary form of divide and rule. Perhaps there's something to be said of the predictive capacities of big data and AI, like the stories that technology can finally identify 'harmful' trends and intervene accordingly, that ensures the appeal of a 'saved by science' model to anxieties otherwise inevitable calamities. Such preventive imaginings complement a riven social world. This thinking returns us to Mayhew and the 'dangerous classes' of 18th century London.[93] If the state can identify and predict sites of danger, but fails to make us safe even so, then we turn to other more radical dualities which want to prevent the flow of humanity so that we can secure our own small safe spaces.

Two regulatory obligations arise in the climate of anxiety. First is a general responsibility on politicians and policy makers to keep the control discourse within objective and evaluative boundaries. An example of this is the daily, detailed public reporting from the Singapore Ministry of Health concerning the demographic details of infection rates, tracing programmes, hospitalisation and community re-integration. This exemplary information flow was not so well maintained when the Qr Code safe-entry strategy was rolled out (with detailed explanation about the centralisation of data only advertised on a government website).[94] Second is the obligation on social media news platform providers and press councils covering conventional media professional standards to vigilantly oversee balanced reporting and not only identify and redact fake news.

Individual and Data Integrity

---

[92] We accept that because there are genuine scientific and control-centered disputes about information and outcomes, evidenced-based policy will always be a casualty in an emerging and evolving crisis such as the current pandemic.

[93] Henry Mayhew, *London Labour and London Poor* Ware: Wordsworth Editions (2008).

[94] The Safe Entry website explains the following: "All data is encrypted, and the data can only be accessed by authorised personnel for contact tracing purposes. The data will be purged when it is no longer needed for contact tracing purposes. Under the Public Sector Governance Act, public officers who recklessly or intentionally disclose the data without authorisation, misuse the data for a gain, or reidentify anonymised data may be found guilty of an offence and may be subject to a fine of up to $5,000 or imprisonment of up to 2 years, or both.
The data collected via SafeEntry is stored in the Government server, which will only be accessed by the authorities when needed for contact tracing purposes. The Government is the custodian of the data submitted by individuals, and there will be stringent security measures in place to safeguard access to personal data. Only authorised public officers involved in contact tracing will have access to the data, when the need arises. The data may also be de-identified and aggregated for analytics purposes.
Contact data will be shared with the relevant authorities for the specific purpose of contact tracing."
See "How will my data be protected", Safe Entry website <https://support.safeentry.gov.sg/hc/en-us/articles/900000681226--How-will-my-data-be-protected-> (accessed 22 May 2020)

It is important to ensure that data is genuine and fit for the declared purpose, particularly if that emergency purpose I meant to justify abnormal data intrusion. Its objective will be defeated, and unnecessary risk can arise if data that goes into or out of say a tracing app is inaccurate. Further, if the app advertisers a purpose that it cannot achieve through insufficient data coverage, citizens may become complacent and ignore alternative control measures with a better record of success. Imagine the consequences for eroding trust, of sending out a hundred notifications or requests for self-quarantine on the basis of an incorrectly recorded contact, or as happened recently, notifications of positive tests when the test results were faulty. Therefore, data integrity, or the maintenance of, and the assurance of the accuracy and consistency of data over its entire life-cycle, is a critical requirement for the design, implementation and usage of any system which accesses, stores, processes, or retrieves personal data like the case in point.[95]

In the preferred regulatory attribution it would be the responsibility of the technology promoter, the data-harvester, and the data user to have design requirements, and data verification fail-safes so that the harmful consequences of inaccurate (or incorrectly analysed data) are minimised and monitored (If the ESU model is adapted this would be the unit's regulatory responsibility).

A completely anonymous data facility where data accuracy is not independently verified can be prone to error and possible abuse. Under the guise of anonymity, users may submit inaccurate information in bad faith, or in good faith but incompetently. To solve the problem of tainted data and the problematic consequences that it represents for individual's liberties and integrity, data protection regulators (specifically, in the self-regulatory mode, the app promoters) should encourage and embrace the implementation of independent verifiers for the apps that are implemented in COVID-19 related controls, but at the same time not compromising the integrity of the data in use (The CPDC would provide that independent verification). This would be an *ex ante* measure that may help governments to preserve data integrity, achieve control purposes, and better ensure data subject trust through accountability mechanisms.

However, data integrity also requires some es post controls once the app is functioning and a possible inaccuracy has been detected. We suggest to that preferred data protection authorities (and as a first stage responsibility, app promoters) develop a set of KPIs that public and private authorities KPIs to assess and reflect the effectiveness of the apps in supporting contact tracing. This measure was suggested by the European Commission in April 2020. However, the European Commission does not address which authority should be in charge of this ex post measure.[96] In keeping with the specific responsibilities for promoters they should propose KPIs overseen by the CPDC.

---

[95] Kevin H. Govern and John Winn, *Data Integrity Preservation and Identity Theft Prevention: Operational and Strategic Imperatives to Enhance Shareholder and Consumer Value*, RISK MANAGEMENT AND CORPORATE GOVERNANCE, ABOL JALILVAND AND A. G. MALLIARIS, ED., ROUTLEDGE (2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128834>

[96] European Commission, "E-Health Network, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States" (15 April 2020) <https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf>

Accessibility

Much emphasis has been placed on universal application and the digital accessibility of control strategies and technology. Particularly in South World locations, reliance on smartphone technologies for participation in control efforts will discriminate against those without access to this technology, and cause anxiety if citizens believe their safety is at risk through non-participation. The same is the case with elder populations that are less technologically capable. These disadvantages need to be recognised and at least alternative manual engagement should be offered by app promoters where possible.

The greatest accessibility issue at the centre of alleviating the crisis is vaccine availability and coverage. Many teams are currently at work on producing a vaccine and China has pledged a massive manufacturing capacity to make available vaccine advantage world-wide.[97] Universal access to vaccination when it eventuates is the prime example of a need for international regulatory cooperation and nation-state interventions against intellectual property barriers. Some of the best placed teams to reach vaccine certification are subsidised by large pharmaceutical companies.[98] One of these organisations at least has promised to charge out doses at cost for the life of the pandemic.[99] This on its own is insufficient assurance that the COVID-19 vaccine will not go the way of HIV-Aids medication, and be available only to the rich. International philanthropic organisations have a role to play in shaming rabid commercialisation and profiteering. National legislatures and courts have the tools of price-fixing and compulsory licensing to counter commercial inaccessibility.[100] Social justice over profit protection is recognised in international trading agreements for circumstances such as these.[101]

Challenges Associated with authority/legitimacy and accountability

Private sector data sharing

One tool in the data privacy legislation toolbox is "information fiduciary" rules. The basic idea is this: When you give your personal information to a data collector or data processor in order

[97] Corinne Gretler, "Xi Vows China Will Share Vaccine and Gives WHO Full Backing", *Bloomberg* (19 May 2020) <https://www.bloomberg.com/news/articles/2020-05-18/china-s-virus-vaccine-will-be-global-public-good-xi-says> (accessed 20 May 2020)

[98] Ara Darzi, "The race to find a coronavirus treatment has one major obstacle: big pharma", *The Guardian* (2 April 2020) <https://www.theguardian.com/commentisfree/2020/apr/02/coronavirus-vaccine-big-pharma-data> (accessed 20 May 2020)

[99] Zia Sherrell, "Experts weigh in on how much a dose of a successful coronavirus vaccine could cost", *Business Insider* (4 May 2020) <https://www.businessinsider.sg/how-much-will-coronavirus-vaccine-cost-2020-5?r=US&IR=T> (accessed 20 May 2020)

[100] Zia Sherrell, "Experts weigh in on how much a dose of a successful coronavirus vaccine could cost", *Business Insider* (4 May 2020) <https://www.businessinsider.sg/how-much-will-coronavirus-vaccine-cost-2020-5?r=US&IR=T> (accessed 20 May 2020)

[101] David P. Fidler, *Negotiating Equitable Access to Influenza Vaccines: Global Health Diplomacy and the Controversies Surrounding Avian Influenza H5N1 and Pandemic Influenza H1N1*, PLoS Medicine 7(5): e1000247 (2010) <https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1000247>

to get a service, that company should have a duty to exercise loyalty and care in how it uses that data. Professions that already follow fiduciary rules—such as doctors, lawyers, and accountants—have much in common with the online businesses that collect personal data. Both have a direct relationship with customers; both collect information that could be used against those customers; and both have one-sided power over their customers or data subjects.[102]

Accordingly, some have proposed adapting these venerable fiduciary rules to apply to online companies that collect personal data from their customers.[103] New laws would define such companies as "information fiduciaries."[104] Some authors have even proposed to abandon the "one size fits all approach" in data governance when private organisations work with aggregated data collected from individuals who trust in these companies. For those authors, the power that stems from aggregated data should be returned to individuals through the legal mechanism of trusts. Bound by a fiduciary obligation of undivided loyalty, the data trustees would exercise the data rights conferred by the top-down regulation on behalf of the Trust's beneficiaries. The data trustees would hence be placed in a position where they can negotiate data use in conformity with the Trust's terms, thus introducing an independent intermediary between data subjects and data collectors. Unlike the current 'one size fits all' approach to data governance, there should be a plurality of Trusts, allowing data subjects to choose a Trust that reflects their aspirations, and to switch Trusts when needed.[105]

Hence, when the private sector is leading the technology initiatives for controlling the pandemic, privacy can and should be thought of as enabling trust in our essential information relationships. A fiduciary duties approach may empower consumers, build trust and clarify that private companies helping to tackle the virus are also liable not only before health authorities, but as fiduciaries as well. However, this approach requires sophisticated courts and an efficient judiciary system able to adequately enforce those fiduciary duties.

Additionally, in the context of COVID-19 and pandemic control, regulators (such as the CDPC and specific application and technology ESUs), should also consider setting up a national system of evaluation/accreditation endorsement of national apps. This will add an ex-ante protection mechanism for data subjects who will be able to discriminate among the multiple offers of surveillance/tracing technologies available in a specific jurisdiction.

---

[102] Sylvie Delacroix and Neil Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, FORTHCOMING IN INTERNATIONAL DATA PRIVACY LAW (2018). <https://ssrn.com/abstract=3265315>

[103] Adam Schwartz and Cindy Cohn, "Information Fiduciaries" Must Protect Your Data Privacy, Electronic Frontier Foundation (25 October 2018) <https://www.eff.org/es/deeplinks/2018/10/information-fiduciaries-must-protect-your-data-privacy>; Neil Richards and Woodrow Hartzog, *Taking Trust Seriously in Privacy Law,* 19 STANFORD TECHNOLOGY LAW REVIEW 431 (2016) <https://law.stanford.edu/wp-content/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf>

[104] Gennie Gebhart, "EFF's Recommendations for Consumer Data Privacy Laws", Electronic Frontier Foundation (17 June 2019) <https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws> (accessed 19 May 2020)

[105] Sylvie Delacroix and Neil Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, FORTHCOMING IN INTERNATIONAL DATA PRIVACY LAW (2018). <https://ssrn.com/abstract=3265315>

State sector surveillance

The main promoters of surveillance technologies in the current crisis are state health agencies. The UK and Australian experiences with rolling out contact tracing apps have highlighted two areas of state power that are contentious. The first relates to volition or compulsion when it comes to app up take. This choice was debated at length in the Australian context and against a variety of civil rights and community trust measures, compulsion was not preferred.[106] We concur with these arguments and hold in any case that the reality of informed and actual consent in situations such as the one in question are of themselves sufficiently problematic as to make comfort drawn from volition, cold and conditional.

The second issue involves data repositories. Several models prefer that data should be stored centrally, assuming in some state repository.[107] The problems associated with this from a data protection point of view are so obvious as to not require detailing. The other alternative is that all data remains on the individual device and this is said to offer maximum privacy protections. This assertion has also been disputed.[108]

The starting point for the European Data Protection Board Guidance for COVID-19[109] is that contact tracing apps should be voluntary and not rely on tracking individual movements based on location data but on proximity information regarding users (e.g., contact tracing by using Bluetooth). Especially noteworthy is that the EDPB stresses that such apps cannot replace but only support manual contact tracing performed by qualified public health personnel, who can sort out whether close contacts are likely to result in virus transmission or not. The proximity emphasis, and need for manual tracing to predominate, is not consistent with applications for entry screening operated by employers to track the entry and egress of employees and suppliers to places of work.

Whichever position prevails on voluntary/compulsory and centralised/individualised, state-sponsored surveillance through the application of intrusive technologies is not a regulatory challenge that can be adequately met either by self-regulation or through community activism. This is one occasion where the governance of an independent and commensurably powerful independent data protection agency is to be preferred.

---

[106] Amanda Meade, "Australian coronavirus contact tracing app voluntary and with 'no hidden agenda', minister says", *The Guardian* (18 April 2020) <https://www.theguardian.com/technology/2020/apr/18/australian-coronavirus-contact-tracing-app-voluntary-and-with-no-hidden-agenda-minister-says> (accessed 20 May 2020)

[107] Under the centralised model, the anonymised data gathered is uploaded to a remote server where matches are made with other contacts, should a person start to develop Covid-19 symptoms. This is the method the UK, is pursuing. Singapore and Australia adopted the centralised model as well. Cristina Criddle and Leo Kelion, "Coronavirus contact-tracing: World split between two types of app", *BBC News* (7 May 2020) <https://www.bbc.com/news/technology-52355028> (accessed 20 May 2020)

[108] Joe Duball, "Centralized vs. decentralized: EU's contact tracing privacy conundrum", *International Association of Privacy Professionals* website (28 April 2020) <https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/> (accessed 20 May 2020)

[109] European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (21 April 2020) <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>

Challenges associated with good governance and data justice

Foreword to this section is the universal preference that if data surveillance technologies, tracing, tracking, safe entry or quarantine processes are instituted by the state they should rest on democratically debated legislative authority. Such authority is not satisfied, except in extreme circumstances by relying on general emergency powers or by broadly enunciated health and safety, national security, immigration or public order provisions. In the present control circumstances, many of these initiatives will be augmented from pre-COVID powers to exercise health and safety protections. If so, the particular COVID-19 applications require (for transparency and accountability to be prioritised) specification and not just as administrative provisions under the broad authority of the executive.

In addition, state agencies wishing to avail themselves of such powers must recognise the force and application of constitutional rights and liberties, as well as the specific influence of domestic data protection enactments. Regional and international agreements and conventions which are binding on the activating states must also be taken into account.

As regards the exercise of extra-ordinary data sharing between the private and public data platforms, general use consent provisions, non-specific contract exclusions or commonly worded (and user reliant) privacy statements need to be revisited with special reference to the new sharing practices. These arrangements need to be brought to the individual attention of customers, clients and consumers whose personal data is affected by these sharing protocols.

Compliance with legislative power provisions, private contract obligations and international best practice are fields of review appropriate to the work of the independent data protection agency. A public complaints facility may have the capacity to sharpen this review and increase public confidence in the regulator.

Explainability

Much of what would be discussed under this sub-heading has already been canvassed in considerations of transparency and accountability. We see community comprehension as essential for informed consensus, voluntary participation and the active investment of trust. The first regulatory attribution here rests with the promoters of the device or data users (If ESUs are employed they would coordinate this responsibility). Explainability is more than just the provision of complex and comprehensive information. It needs to be confirmed through evaluations of genuine understanding. Civil society has an important role in testing and confirming that risks and benefits have been comprehensively explained. Many reservations on trusting control strategies and data use are based on misinformation, incomplete information, double meanings or counter-messages. An effective way to measure whether the message is getting through and it is the intended message, is through public complaints functions. It is envisaged that this remit in the CPDP's brief will provide an important and independent verification tool when explainability is in question.

Avoiding bias

In some cases, biases can manifest as a result of challenges associated with data governance. For instance, certain location data is scattered among multiple commercial platforms generated by automatic location notifications, producing personal movement data about which most data subjects are not even aware. Bigtech companies can also collect location data and have enormous reach within the population.[110] Any kind of automated contact tracing that hopes to find the total array of close contacts will need to access more than a thin slice of existing data pools if the tracking is to effectively find otherwise unknown infected people. In addition, if location data is available to augment proximity data then there is a case for its limited and responsible use. However it should be remembered that location information provided for one purpose but used for another can, and often does generate biased analysis. For instance, if someone uses their smartphone locator to traverse Google maps and enters premises where a gay night club may also be operating, if that information is connected with health safety tracing, the nature of the data subject's contexts will carry an assumed bias until manually corrected. Data sources may represent a problem of false conclusions and unsubstantiated analysis which eventuates in misrepresentations of certain associations, and thereby magnifying biases. There may also be differences in how various populations and demographics are represented in the data from one location motivation to another. Making public health decisions on such datasets could leave out entire populations, misrepresent others, and lead to a deployment of health care resources that is ineffective from a public safety standpoint.[111] The originating regulatory attribution again rests with the technology promoter and data user to work with designers in identifying possible algorithmic bias and countering it as the technology is developed. Bias generation needs then to be constantly monitored against the datasets and databases combined in mass data use from unconnected purposes, to health safety tracing objectives.

Data aggregation is not enough

[110] An example being Facebook. Facebook's Data for Good program is developing Disease Prevention Maps, which show how people are moving around regions. Facebook hopes this data can be used alongside other information that public health officials collect to help determine areas where COVID-19 outbreaks are likely to occur. According to Facebook, the maps include: Co-location data, movement range trends and a social connectedness index. Christina Farr, "Facebook is developing new tolls for researchers to track if social distancing is working", *CNBC* (6 April 2020) <https://www.cnbc.com/2020/04/06/facebook-to-help-researchers-track-if-social-distancing-is-working.html> (accessed 20 May 2020)
With over 2.6 billion monthly active users as of the first quarter of 2020, Facebook is the biggest social network worldwide. In the third quarter of 2012, the number of active Facebook users surpassed one billion, making it the first social network ever to do so. "Number of monthly active Facebook users worldwide as of 1st quarter 2020", *Statista* website https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (accessed 20 May 2020)

[111] Jay Stanley and Jennifer Stisa Granick , "The Limits of Location Tracking in an Epidemic", American Civil Liberties Union (8 April 2020) <https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf> (accessed 19 May 2020)

At the most basic level, there's a fundamental, operational difference between "aggregated" location data and "anonymized" or "deidentified" location data.[112] Compared to using individualized location data for contact tracing—as many governments around the world are already doing—deriving public health insights from aggregated location data poses fewer privacy and other civil liberties risks such as restrictions on freedom of expression and association. However, even "aggregated" location data comes with potential risks and pitfalls. Indeed, aggregation is not a synonym of anonymisation. There's a difference between "aggregated" location data and "anonymized" or "deidentified" location data. Information about where a person is and has been itself is usually enough to reidentify them. Someone who travels frequently between a given office building and a single family home is probably unique in those habits and therefore identifiable from other readily identifiable sources.[113] A study from 2013 found that researchers could especially characterize 50% of people using only two randomly chosen time and location data points.[114] Will preserving privacy when using aggregated data depend on other temporal and spatial factors around when and how the data aggregated? How large of an area does each data count cover so important associations cannot be drawn but extraneous connections can be avoided? When is a count considered too low and dropped from the data set?[115] For example, injecting statistical noise into a data set preserves the privacy of data subjects, but might undermine the accuracy of the decisions taken based on the particular data set.[116] Each of these questions are indicative of how complex it is to rely on data anonymity as a source of individual protection. These variables should be widely known and discussed when any justification relying on aggregation or anonymity is advanced.

In order to address the potential risks and limitations of data aggregation, it is necessary to implement some high-level practices personal data management practices in the fight against COVID-19.[117] First, private or public companies that produce reports based on aggregated location data from users should release their full methodology as well as information about who these reports are shared with and for what purpose. To the extent they only share certain data with selected "partners," these groups should agree not to use the data for other purposes or attempt to re-identify individuals whose data is included in the aggregation. Again, this private sector use compliance can be monitored by informed civil society and when shortfalls from best practice arise, the independent agency can investigate and intervene,

---

[112] Sophie Stalla-Bourdillon and Alison Knight, *Anonymous Data v. Personal Data — A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, WISCONSIN INTERNATIONAL LAW JOURNAL (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2927945>

[113] Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19", Electronic Frontier Foundation (6 April 2020) <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed 19 May 2020)

[114] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen & Vincent D. Blondel, *Unique in the Crowd: The privacy bounds of human mobility,* SCIENTIFIC REPORTS VOLUME 3, ARTICLE NUMBER: 1376 (2013) <https://www.nature.com/articles/srep01376>

[115] Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19", Electronic Frontier Foundation (6 April 2020) <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed 19 May 2020)

[116] An Nguyen, "Understanding Differential Privacy", *Towards Data Science* (1 July 2019) <https://towardsdatascience.com/understanding-differential-privacy-85ce191e198a> (accessed 20 May 2020)

[117] Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19", Electronic Frontier Foundation (6 April 2020) <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed 19 May 2020)

particularly if any breach involves the monetising of secondary data. Second, data aggregators need to disclose how they address the trade-offs between privacy and granularity and usefulness of data sets. Third, there's often pressure imposed on data aggregators to reduce the privacy properties in order to generate an aggregate data set that a particular decision-maker claims must be more granular in order to be meaningful to them.[118] Before moving forward with plans to aggregate and share location data, aggregators should consult with independent experts approved by the protection agency about the aforementioned trade-offs. Getting input on whether a given data-sharing scheme sufficiently preserves privacy can help reduce the bias that such pressure creates.[119] Use-case evaluations on particular balancing considerations (protection of privacy and protection of public safety) would come within the independent agency's arbitration function.

Privacy by design is not enough

Tech solutionism and privacy-by-design might not be enough for addressing the challenges associated with good governance and data justice. The current focus of the privacy community is very much on whether such apps meet the principles of privacy by design.[120] However, privacy by design is actually embedded within the processes of most companies who have recently come under scrutiny for suspect privacy practices.[121] This begs the question whether privacy by design is enough, beyond expressions of good intent to actually translate into monitored best practice. The inadequacies of privacy by design speak volumes in justifying the higher positioning of an independent protection agency in the COVID-19 personal data protection pyramid, above the self-regulatory endeavours of designers, promoters and users.

The main challenge to effective privacy by design is that business concerns often compete with and overshadow privacy concerns. In other words, privacy by design only goes as far as the organization culturally and commercially accepts it.[122] Hence, in an enforced self-regulation spirit, designers and promoters need to work with independent regulators to agree much clearer guidance about applicable design principles and how best to incorporate them into software development processes in practice. Greater guidance is also needed about how to balance privacy with business (or eventual public safety) interests, and there must be

[118] Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19", Electronic Frontier Foundation (6 April 2020) <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed 19 May 2020)

[119] Jacob Hoffman-Andrews and Andrew Crocker, "How to Protect Privacy When Aggregating Location Data to Fight COVID-19", Electronic Frontier Foundation (6 April 2020) <https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19> (accessed 19 May 2020)

[120] Organisation for Economic Co-operation and Development (OECD), "Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics", *OECD Policy Responses to Coronavirus (Covid-19)* (23 April 2020) <http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/> (accessed 20 May 2020)

[121] Ira Rubinstein and Nathaniel Good, Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents,* 28 BERKELEY TECHNOLOGY LAW JOURNAL 1333 (2013), NYU SCHOOL OF LAW, PUBLIC LAW RESEARCH PAPER NO. 12-43 (2014) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128146>

[122] Lauren Kaufman, "Is 'Privacy by Design' Enough? Product development's privacy alibi", *Medium, Popular Privacy* (20 January 2020) <https://medium.com/popular-privacy/is-privacy-by-design-enough-12aa4fddb747> (accessed 20 May 2020)

oversight mechanisms, such as an independent agency, in place. Tech-driven initiatives must be aligned with trust-based business strategies with stakeholder accountability metrics to overcome trust redaction from many citizens and consumers located on brands and institutions. Corporate culture should be part of what data protection regulators oversee from a privacy perspective, consistent with the enforced self-regulation model.

Cybersecurity

Ransomware attacks on hospitals and health systems have continued during the pandemic, raising key cybersecurity considerations about infrastructure disruptions.[123] COVID-19 has caused governments and private companies to spread and dilute data security priorities and resources, making it even more challenging to get attention focused on addressing cybersecurity challenges like ransomware attacks, which have been significant issues to healthcare cybersecurity even before the pandemic.[124]

The technology-driven solutions for contact tracing and surveillance have become an important feature of the strategies for a return to the "new normal". However, this tech-driven trend might be exposing data subjects and health system stability in ways that have not been factored into risk/benefit analysis. The issue at the security level is not simply whether there is a misplaced confidence in the capacity of tracing apps to balance out added health and safety compromises through a reduction in self-distancing, although this must be vigorously reviewed if automated tracing is to offer anything but a false sense of security. Governments and private organisations deploying this type of solutions often talk about the importance of nominated technology for saving lives. Coincidentally there has not been in these justifications disclosure on how citizens in this new environment are exposed to insecurity more than the inherent over-expectations for the tech. It has been reported that the government's anticipated COVID-19 tracing app in the UK has failed crucial security tests and is not yet safe enough to be rolled out across the country.[125] It is understood the system has botched all tests needed in order for it to be encompassed in the NHS Apps Library, including cyber security, clinical safety and performance.[126] Until these regulatory and quality control hurdles can be met then there is little point in standardisation of cyber security protocols, when emergency exceptions avoid their universal ascription.

---

[123] Jackie Drees, "COVID-19 cyber threats: Why data integrity is crucial & how to protect it", *Becker's Health IT* (6 May 2020) <https://www.beckershospitalreview.com/cybersecurity/covid-19-cyber-threats-why-data-integrity-is-crucial-how-to-protect-it.html> (accessed 20 May 2020)

[124] For example, the most serious breach of personal data in Singapore's history took place in 2018, with 1.5 million SingHealth patients' records accessed and copied while 160,000 of those had their outpatient dispensed medicines' records taken. Kevin Kwang, "Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted", *Channel News Asia* (18 October 2018) <https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyberattack-pm-lee-target-10548318> (accessed 21 May 2020)

[125] lex Lynn, "COVID-19 tracing app fails NHS and cyber security tests", Electronic Specifier (6 May 2020) <https://www.electronicspecifier.com/industries/medical/covid-19-tracing-app-fails-nhs-and-cyber-security-tests> (accessed 19 May 2020)

[126] Alex Lynn, "COVID-19 tracing app fails NHS and cyber security tests", Electronic Specifier (6 May 2020) <https://www.electronicspecifier.com/industries/medical/covid-19-tracing-app-fails-nhs-and-cyber-security-tests> (accessed 19 May 2020)

If governments would like for people to opt into such applications, they need to address universal security concerns. To achieve this result, cybersecurity authorities should disclose to the public if the apps used for containing the pandemic comply with the same standards that other health data processing initiatives observe.

Expiration of the use of data

Massive collections of data could help curb the COVID-19 pandemic. However, 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. Essential in any best practice menu is the expiration and redaction of data once the purpose for its collection has been met. In so saying we return to a fundamental expectation that emergency purposes are clearly enunciated, contained and achievable.

The pandemic crisis that the world is facing because of the COVID-19, and its immediate and unabated containment, are being used to justify extraordinary personal data-harvesting and data sharing, in the short term. At the same time that surveillance is argued as a paramount public health safety priority, 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.

Personal data kept after the lockdown has been lifted is likely to be kept for longer than originally proposed and will be repurposed. For that reason, it is of utmost importance to have a clear plan for the permanent expunging and erasure of all personal data collected during the pandemic once it no longer serves the original need. It is important to remember that genuinely anonymous information (argued as can never be traced back to the data subject) is not classified in many protection instruments as personal data and, for instance, is not covered by the GDPR. Even so, such anonymised data will exponentially lose its emergency purpose and therefore on that test alone is a candidate for automatic redaction.

It might be argued that, users should have the choice of whether to opt-in to every new use of their data or remain outside the strategy, but we recognize that obtaining consent for aggregating previously acquired location data to fight COVID-19 may be difficult with sufficient speed to address the public health need. Expediency also means that real and informed data subject consent may in practice, be illusory. That's why it's especially important that users should be able to review and delete their data at any time.[127]

Whatever legislative powers are granted to generate, store access and share, either in general form, or more specifically enunciated, they should be contained through sunset clause provisions. Recognising that if the virus crisis has yet to benefit from a deliberative end,

[127] Gennie Gebhart, "EFF's Recommendations for Consumer Data Privacy Laws", Electronic Frontier Foundation (17 June 2019) <https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws> (accessed 19 May 2020)

sunset clauses may be conditional but at least they are an expression of expiration and that is to be commended.

Sunsetting is when a piece of regulation, legislation, agency or program expires at a specific date. It is written into the empowering legislation or administrative guideline in the form of a sunset clause. Sunset clauses can make provision for future review. The goal is to force the rule-maker to revisit the regulation to determine whether it should be extended automatically expire.[128]

Sunsetting is often, but not always, associated with emergency legislation that is enacted during war and other times of crises. For example, the 2001 US Patriot Act and 2005 UK Prevention of Terrorism Act include sunset clauses.[129] In line with this trend, a few countries have included or considered sunset clauses as part of their response to COVID-19.

About 100 countries so far have declared states of emergency due to COVID-19.[130] These states of emergency give the government additional powers, for example to restrict movement (e.g. for quarantines), collect personal information (e.g. for contact tracing), requisition resources like masks and care facilities, dissolve parliament, postpone elections, and more. These laws give governments exceptional powers to respond to exceptional circumstances but could have negative implications for people's rights to privacy, freedom of assembly, and property.

In response, jurisdictions including the UK, Ireland, Scotland and France have incorporated sunset clauses into their COVID-19 emergency legislation. In the UK, for example, section 89 of the Coronavirus Act affords that the majority of provisions will expire after two years. Section 98 further states that the Act must be renewed in parliament every month.[131] In Ireland, The Health Act 2020 will expire on 9th November 2020 unless parliament specifically extends it. In Scotland, the Coronavirus (Scotland) Act will expire after six months. The Act may be extended for two six-month periods. In France, the emergency bill will expire within two months unless it is extended.[132]

In practice, sunsetting is not always an effective expiration device. One common shortcoming is that the targeted regulation receives "rubber stamp" re-approval, as opposed to meaningful review. For example, part 4 of the UK 2001 Anti-terrorism, Crime and Security Act

---

[128] Sofia Ranchordas, Sunset Clauses and Experimental Regulations: Blessing or Curse for Legal Certainty?, STATUTE LAW REVIEW 36, NO. 1 PG. 28–45 (2015) <https://academic.oup.com/slr/article-abstract/36/1/28/1614369?redirectedFrom=fulltext>; Ittai Bar-Siman-Tov, Temporary Legislation, Better Regulation, and Experimentalist Governance: An Empirical Study, REGULATION & GOVERNANCE 12, NO. 2 Pg. 192–219 (2018) <https://doi.org/10.1111/rego.12148>

[129] Sofia Ranchordas, Sunset Clauses and Experimental Regulations: Blessing or Curse for Legal Certainty?, STATUTE LAW REVIEW 36, NO. 1 PG. 28–45 (2015) <https://academic.oup.com/slr/article-abstract/36/1/28/1614369?redirectedFrom=fulltext>;

[130] Christian Bjornskov and Stefan Voigt, "The State of Emergency Virus", *Verfassungsblog (blog)* (19 April 2020) <https://verfassungsblog.de/the-state-of-emergency-virus/> (accessed 15 May 2020)

[131] "Coronavirus Act 2020", *Statute Law Database website*, <http://www.legislation.gov.uk/ukpga/2020/7/contents> (accessed 15 May 2020)

[132] Sean Molloy, "COVID-19, Emergency Legislation and Sunset Clauses", UK Constitutional Law Association Blog (8 April 2020) <https://ukconstitutionallaw.org/2020/04/08/sean-molloy-covid-19-emergency-legislation-and-sunset-clauses/> (accessed 22 May 2020)

allows for indefinite detention of non-national terrorist suspects. The Act was reviewed in 2003, but with little scrutiny.[133]

It is anticipated that use cases will arise where automatic data expiration needs to be reviewed. Provided the conditions for and consequences of the review are open, and the data subject is empowered to participate in the review, then individual evaluations of data life extension appear appropriate.

[133] Sean Molloy, "COVID-19, Emergency Legislation and Sunset Clauses", UK Constitutional Law Association Blog (8 April 2020) <https://ukconstitutionallaw.org/2020/04/08/sean-molloy-covid-19-emergency-legislation-and-sunset-clauses/> (accessed 22 May 2020); Gary E Marchant, Braden R Allenby, and Joseph R Herkert, THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM, vol. 7, 2011 (Springer Science & Business Media: Netherlands)