7-2021

COVID-19 responses: A living archive

Centre for AI & Data Governance (SMU)

COVID-19 Responses: A Living Archive

A Compendium by the

Centre for AI & Data Governance (SMU)

Yong Pung How School of Law
Singapore Management University
55 Armenian Street
Singapore 179943

www.caidg.smu.edu.sg

Published in Singapore

First published July 2021

ISBN 978-981-18-1782-3

Table of Contents

1. Editors' preface

1.1 Compendium's mission and aims

COVID-19 has reshaped our lives, the global economy, and the geopolitical landscape in unimaginable ways. Socio-economic disruptions are keenly felt across every sector in every country and irreversible damage has been done to our collective health and livelihood opportunities. From a health crisis, the pandemic has insidiously unfolded into a human one - where efforts taken to contain the virus have resulted in the targeting and/or neglect of vulnerable populations, the exacerbation of structural inequalities, and the pushback against fundamental rights and freedoms. The prolonging of this health crisis has also accentuated the need for better governance as questions of ethical compliance (including its lack thereof) and complicity arise. Yet, it remains important that we do not lose sight of our strength in this period of adversity. In precious moments where we are able to witness our innate human resilience and capacity to thrive in the face of this unprecedented health (political and economic) crisis, we must consider ourselves so fortunate.

This compendium draws together a collection of some of the research produced by the Singapore Management University's Centre of Artificial Intelligence & Data Governance during the course of this health crisis. The included papers seek to showcase the sum of our thinking on critical AI governance issues that have emerged in this pandemic as a result of State control approaches and responses. In putting together this series, our editorial goal is a simple but worthy one: we endeavour to provide our readers with an accessible understanding of the evolving COVID-19 related issues to inspire policy and regulatory refinement for future pandemic governance.

We have pulled together seven papers for this collection. While written at different stages of the pandemic over the past year, the papers speak to many broadly overlapping themes ranging from: the creation and retention of trust in emerging technologies and big databases; the source of authority, use of power, and legitimacy of the state in its pandemic-handling approaches; the concept of vulnerability as inherent in the human condition; the role of ethics in control responses and COVID-19 surveillance strategies; the critical function of regulation and the rule of law; and the increasing need for democratic participation and inclusion in regulatory design and policymaking. While each of these issues are important in their own way, we hoped to emphasize the ways in which these themes arose repeatedly over the course of the pandemic so as to suggest steps towards better and stronger governance.

1.2 Content

In the first paper of this series, *Ethics, AI, Mass Data and Pandemic Challenges: Responsible data use and infrastructure application for surveillance and pre-emptive tracing post-crisis* (the "**Ethics paper**"), Findlay, Loke, Remolina and Tham argue that mass scale surveillance deployed during the pandemic have serious ethical and regulatory implications in the medium and long term in relation to individual dignity, civil liberties, transparency, data aggregation, explainability and other governance challenges. The analysis also looks at data protection and citizen integrity and reflects on other surveillance methods outside the health context, such as initiatives implemented in the financial sector, where similar challenges have arisen.

Building on the Ethics paper, in *Regulating Personal Data Usage in COVID-19 Control Conditions* (the "**Covid Regulation paper**"), Findlay and Remolina calls for regulation that recognises crisis exigencies, reflects on personal data challenges, before surveying policy and regulatory options to equitably address the challenges faced during the pandemic.

COVID-19 Vaccine Research, Development, Regulation and Access (the "**Vaccine paper**"), came at a time where governments were engaging in potential COVID-19 vaccination. Tham and Findlay map developments in the vaccine race and reflect on the way that political, commercial, hegemonic and humanitarian realities will influence law's regulatory relevance particularly through intellectual property regimes. Drawing on existing intellectual property protections, the paper argues that a state cannot rely on the best intentions of successful manufacturers to promote social good when profits are potentially significant and market competition is constrained. The political and economic externalities pressuring more socially responsible commercial decision-making in the vaccine case are unique but even so law's normative framework for justice and fairness is a counterbalance to private property exclusion when world health is at stake.

The Centre's research also includes a deep dive into sector specific issues. In her paper, *Towards a Data-Driven Financial System: The Impact of COVID-19* ("**the Financial System paper**"), Remolina explores the impact of the COVID-19 outbreak on the global economy and the financial sector, which plays a critical role in mitigating the unprecedented macroeconomic and financial shock caused by the pandemic. Financial regulators and supervisors, central banks, along with governments and legislatures face challenges to maintain economic and market stability, preserve the well-functioning core markets, and ensure the flow of credit to the real economy in this pandemic. This paper explains the ongoing data revolution in the financial services industry and how traditional financial institutions and fintechs are trying to leverage data-driven solutions to respond to the challenges associated with the economic crisis derived from the pandemic. Remolina argues that despite the potential benefits of this transformation, the future of data-driven finance in a post-pandemic world looks challenging and generates many risks for consumers and the stability of the financial sector that regulators need to address. An adequate balance of different regulatory objectives will be crucial for a sustainable recovery in a post-pandemic financial industry.

In another sector specific paper, *Pandemic Paradox and Polanyi: Financial markets rise, economies crash, and regulators toss a coin* (the "**Polanyi paper**"), Findlay examines the current disconnect between the financial markets and the economy as being a story of two different realities. The paper aims to forewarn regulators concerned that these two worlds of global wealth generation and growth are moving to polar opposite futures. Findlay reflects on a legal model for financial markets, their regulation and its limitations so that law and finance may be understood as positively relational when considering market sustainability; and then suggests that the explanation for this dangerous disconnect can be found in Karl Polanyi's understanding of fictitious commodities in self-regulating markets, dis-embedding from the social and his propositions for market correction through the double movement.

Drawing on legal theory principles in *Ethics, Rule of Law and Pandemic Responses* (the "**ROL paper**"), Findlay recounts a growing dissatisfaction with ethics and principled design as either the single or primary self-regulatory regime ensuring responsible data use and trustworthy AI. From this foundation, he proposes rule of law compliance as a parallel and supportive normative and operational direction to address the deficiencies likely in any over-reliance on

ethics regulation. In expressions of resistance to COVID responses, there is scant community confidence in assertions that ethical reflections answer the deeply felt and differentially identified reservations regarding surveillance and data usage in pandemic responses. Without the essence of democratic participation, in the form of citizen connection with emergency policymaking, and potential actionability through legal remedies if rights and liberties are compromised (both features of 'thick rule of law'), then the regulatory legitimacy crisis facing principled regulatory regimes remains.

In the last paper of this series, *AI and Data Use: Surveillance Technology and Community Disquiet in the age of COVID-19* (the "**Disquiet paper**"), Wee and Findlay survey community disquiet in the context of smart technologies deployed during the pandemic. In particular, the paper studies sources of social responses to the different control measures and the escalated use of surveillance technologies. The concerns voiced by citizens underscore their worries surrounding infringement of their rights, liberties and integrity, which the authors examine through six broad themes: disquiet about the data collected; disquiet concerning authority styles confirming control responses; disquiet regarding the integral architecture of control strategies employed; disquiet surrounding infringement of rights and liberties; disquiet surrounding the role of private sector; as well as uncertainties regarding a post-pandemic world and its "new normal". The findings reveal that the resulting distrust of both the surveillance technology and the authorities behind these have a pronounced effect on the technology's utility and accuracy. Ultimately, the paper argues that public confidence in governments' control policies and the technologies that they employ can only be rebuilt through a genuine inclusion, engagement, and collaboration with citizens in the conceptualisation, development, implementation and decommissioning phases.

The chapters in this compendium have been curated in a narrative meant to guide readers to first explore the challenges of the pandemic, mull over the aims and foci that governments ought to bear in mind when enforcing regulations, before providing some suggestions on how to improve existing approaches, stimulating readers to think deeper about future challenges that will arise. Ultimately, we hope to show the importance of the regulatory function of ethics and law in both ensuring the containment of the virus and in safeguarding individual autonomy and human dignity.

Chapter 2 briefly outlines the common responses and strategies employed by state and government officials. Following that, chapter 3 delves into the challenges that have arisen out of the pandemic, including challenges resulting from weak and poor governance efforts. Chapter 4 provides a comprehensive examination of common regulatory pitfalls and offers recommendations on how to safeguard against them. Chapter 5 stresses the importance of modifying current approaches to the pandemic by initially and principally advocating for three normative foundations: avoiding discrimination; compliance with ethical and principled design; and the commitment towards citizen inclusion and engagement. It is asserted that adherence to these normative foundations will help achieve greater public trust and reinforce state legitimacy. Chapter 6 pre-empts the upcoming pandemic specific challenges that authorities ought to anticipate and prepare for. Finally, chapter 7 advocates for a global approach in mitigating a global pandemic which has proven to be vital, in light of existing fragmented jurisdictional practices.

In putting together this compendium, we recognise that different countries experience their unique pandemic-related challenges. As a matter of course, we expect that distinct regulatory requirements and priorities will arise. The compendium does not claim to have an answer to all

of the world's regulatory problems; we do not also envisage that adherence to the solutions offered here will alleviate all of society's control-related hardship. Nevertheless, we hope that our efforts in compiling this book will provide some insights into existing regulatory challenges and guide the reader in their pursuit of understanding, scrutinising, and refining existing pandemic governance and measures for the betterment of society.

1.3 How to use/read the sections

In this compendium, each subsection typically amalgamates points referenced from the seven papers introduced above. Given the uniqueness of this collection, we felt it would be pertinent to explain the stylistic demarcations that are used throughout the book. While each of the cited papers present its own unique questions and can be read as a standalone piece, they are pulled together by common themes. Within each subsection, we group each paper's points together and insert a tilde "~" to denote different papers. Within a particular section, paragraphs that end with bracket ellipsis "(...)" signal to the reader that the subsequent paragraph is quoted from a different section of the original paper, while paragraphs without bracketed ellipses indicate that they were continuous sections of the original paper that have been extracted. Finally, the end of each quoted paper is marked with a square bracket containing the name of the papers they were referenced (e.g. [*Vaccine paper*]).

Wherever relevant, the compendium's editors have also sought to include headers or phrases to help improve the readability of the texts and clarity of the subject matter. All our insertions are marked in square brackets, with all other unmarked headers taken from the original sources. These stylistic signals are inserted to improve the comprehensibility of the text.

As far as possible, we have also kept the excerpts true to their published form and phrasing on SSRN. In so doing, we desire to not only convey the original intention and considerations of the authors at the time of writing, but also, to invite our readers to chart the development of trending concerns throughout the lifecycle of the pandemic. The different focal points of each paper also serve as a poignant reminder that COVID-19 is a fast evolving crisis.

The format of the compendium will illustrate and make evident where our research points have overlapped. In this emphasis, it is hoped that pertinent pandemic-governance issues are highlighted and made prominent to the reader for their personal deliberation. The compendium's content page allows for easy steering through the book should the reader prefer to navigate and pinpoint to a particular interesting issue. The abstracts are in their original form for readers' ease of citation and navigation. We highly encourage readers to engage with the original source for discussions that they are keen to explore further by heading to our website at our Centre's website or via our Research Paper series on SSRN.

Compendium Editors[1]
Jane Loo
Alicia Wee
Sharanya Shanmugam

[1] 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 authors and do not reflect the views of National Research Foundation, Singapore. The editors would like to thank Josephine Seah for her helpful comments on earlier versions of this project.

2. Brief overview of common government responses and strategies

In order to contain the virus, countries around the world have adopted various COVID-19 containment strategies. These include measures such as manual and digital contact tracing, lockdowns, quarantine and isolation, digital check-in systems, and the closure of national borders. This subsection highlights some of the common government responses identified in our previous research and assists the reader in developing an understanding and appreciation of the common COVID-19 control strategies and methods employed.

To combat COVID-19 by achieving a flattening of the curve, most countries have elected to adopt lockdown measures of various extents in order to break the chain of transmission of the Virus. Such lockdown measures include, for example, imposing travel restrictions on foreign visitors, ordering businesses (such as movie theatres, restaurants, bars and pubs) to shut down, factories to stop working, banning mass gatherings (such as large-scale conferences and church congregations), etc.[2] **[*Vaccine Paper*]**

~

The explosion of data-driven citizen surveillance during the pandemic is largely propelled by the unique cooperation of public and private institutions/organisations, which has allowed for a mass scale use of tracking/tracing apps, drones,[3] GPS devices, and facial recognition technologies to permeate mundane situations of movement, association and daily social interaction.[4] Encountering such technology in times of a pandemic (when surveillance is more obvious and apparent than traditional citizen monitoring devices) provides a regular reminder that individuals are being tracked, traced, logged, and aggregated in mass data-sharing practices like never before. Critics remind sponsors and operators of such technology that privacy, data integrity, and civil rights cannot be regarded consequentially as luxuries to be expended owing to the exigencies of the pandemic.[5] (...)

Mass surveillance technologies were a common feature in most global cities, public and private precincts, and transport hubs prior to the pandemic. Wide-scale surveillance has been normalised to such an extent that the upgrading of pandemic surveillance capacity could be achieved without sufficient community engagement and scrutiny if the technology is seen as

---

[2] John Irish and others, 'Lockdowns and Entry Bans Imposed around the World to Fight Coronavirus' *Reuters* (15 March 2020) <https://www.reuters.com/article/us-health-coronavirus-idUSKBN21208S> accessed 23 June 2020.

[3] 'Ronald van Loon on Twitter: "Big #Drone Is Watching You! By @Reuters #Robotics #Security #AI #ArtificialIntelligence #DigitalTransformation Cc: @jblefevre60 @johnlegere @ronald_vanloon @haroldsinnott @mikequindazzi Https://T.Co/Xo1xCMD0I2" / Twitter' (*Twitter*) <https://twitter.com/Ronald_vanLoon/status/1296757198039715840> accessed 21 August 2020.

[4] April 25th and others, 'Covid-19: The Controversial Role of Big Tech in Digital Surveillance' (*LSE Business Review*, 25 April 2020) <https://blogs.lse.ac.uk/businessreview/2020/04/25/covid-19-the-controversial-role-of-big-tech-in-digital-surveillance/> accessed 20 July 2020.

[5] 'We Can Beat the Virus Only By Protecting Human Rights' (*Human Rights Watch*, 6 May 2020) <https://www.hrw.org/news/2020/05/06/we-can-beat-virus-only-protecting-human-rights> accessed 30 July 2020.

just more of the same.[6] For instance, security camera companies who utilise artificial intelligence now boast about their systems' ability to "scan the streets for people with even low-grade fevers, recognise their faces even if they are wearing masks and report them to the authorities."[7] Recently in Singapore, police have pilot-tested automated drones to enforce social distancing measures in public spaces.[8] The exponential use of surveillance technologies by state authorities should generate citizen discussion about whether these control responses would be retained after the threat of the virus has diminished. The extensive and expansive use of such technologies which, in other contexts would likely have presented ethical concerns and immediately trigger community resistance against compromising individual's rights to privacy and autonomy, is now being promoted as essential, inevitable and efficient control responses that would now be irresponsibly ignored by the state and its citizens.[9] ***[Disquiet Paper]***

~

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

In terms of the latter option some examples currently include:

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

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

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

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

---

[6] Marina Motsenok and others, 'The Slippery Slope of Rights-Restricting Temporary Measures: An Experimental Analysis' [2020] Behavioural Public Policy 1.
[7] 'Coronavirus Brings China's Surveillance State out of the Shadows' *Reuters* (7 February 2020) <https://www.reuters.com/article/us-china-health-surveillance-idUSKBN2011HO> accessed 21 July 2020.
[8] 'Ronald van Loon on Twitter: "Big #Drone Is Watching You! By @Reuters #Robotics #Security #AI #ArtificialIntelligence #DigitalTransformation Cc: @jblefevre60 @johnlegere @ronald_vanloon @haroldsinnott @mikequindazzi Https://T.Co/Xo1xCMD0I2" / Twitter' (n 3).
[9] 'Countries Are Using Apps and Data Networks to Keep Tabs on the Pandemic' *The Economist* <http://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic> accessed 4 August 2020.
[10] See Appendix A Table 1 of the *Ethics Paper* on Tracing and surveillance initiatives in different jurisdictions.
[11] Singapore and China case-studies in the *Ethics Paper.*
[12] Singapore and China case-studies in the *Ethics Paper.*

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

3. Challenges arising out of the pandemic

The following subsections will detail some of the challenges that have arisen as a result of the health crisis and the State's endorsement of various pandemic containment measures. The works cited in this chapter invites us to think critically about the efficacy and fairness of common measures employed that may appear neutral or harmless in their initial adoption. Among others, some of the challenges that the papers have observed include the assault on human vulnerability and the exacerbation of discriminatory cycles, risks to privacy and personal data, and the threat to state legitimacy.

3.1 The exacerbation of pre-existing vulnerabilities and cycle of discrimination

The pandemic has had profound impacts beyond that of a health, economic, and political crisis. Our survey of the existing literature has also made apparent how the pandemic has exacerbated existing social inequalities and individual/group vulnerabilities. Certain communities, owing to their vulnerable positioning in society, have found themselves experiencing heightened marginalisation and exclusion. These communities include groups such as migrant workers, the less financially well-off, elderly persons, and racial minorities etc. Discrimination in today's pandemic settings is produced as a result of disproportionate, unfair policies/laws that introduce discriminatory pandemic control/containment measures, or neglect (whether deliberate or unintentional) from state actors and other relevant stakeholders. Discrimination may also arise as a result of reliance on biased and unobjective datasets produced by surveillance technologies employed in this health crisis. On this issue, it is also relevant to note how discrimination is intrinsically linked to the fundamental principle of human dignity.

Discrimination

Despite certain privacy-protecting measures put in place in a number of surveillance contexts, commentators have noted that the data collected, while encrypted and anonymised, can still have the potential to harm certain groups of people, as evident from the pre-emptive monitoring of protests and enforcement measures that clamp down on dissent; a tool that oppressive countries wield to target spots of illegal LGBTQ clubs, or industries that harbour undocumented immigrants.[13] Correlating massive data collection and the subsequent infringement of privacy rights, emphasise the need to know who is controlling and co-ordinating the technology to analyse the data.

Along with surveillance, the European Digital Rights organisation questions the need for "punitive powers of law enforcement" that seek, in theory, to enforce any occurrences of offensive behaviour or violations of social order, consequential to or outside pandemic control reactions. This secondary enforcement application of COVID control data poses a real threat for data integrity, as cities across Europe experiencing the increased pressure of police presence

[13] 'Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit | Michael Veale' (*the Guardian*, 1 July 2020) <http://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights> accessed 30 July 2020.

in their communities at many levels and with varying degrees of intrusion.[14] Law enforcement secondary surveillance purposes complement patterns of selective policing, wherein certain minorities and targeted communities are overpoliced in any event.[15]

Studies have shown that surveillance has a strong tendency to target racialised people, migrants, and the vulnerable sectors of the labour market, all of whom "bear the burden of heightened policing powers and punitive 'public health' enforcement"[16] as they are more likely to have to leave their houses to go to vulnerable work environments no matter what the risks. Their lived realities differ from the privileged individuals who are afforded greater privacy in their ability to work from home and socially distance. [17]

As alluded to above,[18] states have sought to use surveillance data to target marginalised groups i.e. immigrants and LGBTQ clubs. For instance, South Korea has been criticised for using its country's military employing data apps to track down homosexual soldiers.[19] Within the crisis context, Korean LGBTQ citizens voiced opposition to being particularly identified, as they suffered from false rumours about them excessively spreading the virus. Recently, a Korean citizen who visited a series of bars and clubs in the Itaewon district of Seoul tested positive for COVID-19. The Korean media broadcast names of the establishments visited, specifically identifying a gay club, leading to accusations that the LGBTQ community were causing the spread of COVID-19, which subsequently resulted in episodes of harassment of LGBTQ individuals.[20]

In attempts to enforce lockdowns, there are reports regarding disproportionate targeting of ethnic minorities and marginalised groups with violence, unwarranted and unnecessary identity checks, especially in poorer areas of cities.[21] People of colour, indigenous persons and minorities, disproportionately represented in detention and prison populations, where overcrowding serves to catalyse the spread of the virus, are at greater health risk.[22] In urban ghettos, populated on ethnic and racial lines, rates of infection are unequal and intrusive control operations are high. For example, Seine-Saint-Denis, considered one of the poorest urban areas of France populated in majority by immigrants of colour[23] recorded that the number of fines

[14] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (*EDRi*, 27 May 2020) <https://edri.org/surveillance-is-a-pre-existing-condition/> accessed 21 July 2020.
[15] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[16] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[17] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[18] 'Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit | Michael Veale' (n 137).
[19] 'South Korea's Coronavirus Contact Tracing Puts LGBTQ Community under Surveillance, Critics Say' (*The World from PRX*) <https://www.pri.org/stories/2020-05-22/south-korea-s-coronavirus-contact-tracing-puts-lgbtq-community-under-surveillance> accessed 30 July 2020.
[20] Timothy Gitzen, 'Tracing Homophobia in South Korea's Coronavirus Surveillance Program' (*The Conversation*) <http://theconversation.com/tracing-homophobia-in-south-koreas-coronavirus-surveillance-program-139428> accessed 6 August 2020.
[21] 'COVID-19 Lockdown Measures Have Exacerbated Racial Profiling and Police Violence, Says Report' (*The Parliament Magazine*, 29 June 2020) <https://www.theparliamentmagazine.eu/news/article/covid19-lockdown-measures-have-exacerbated-racial-profiling-and-police-violence-says-report> accessed 6 August 2020.
[22] 'COVID-19_and_Racial_Discrimination.Pdf' <https://www.ohchr.org/Documents/Issues/Racism/COVID-19_and_Racial_Discrimination.pdf> accessed 6 August 2020.
[23] 'Policing the Pandemic - Human Rights Violations in the Enforcement of COVID-19 Measures in Europe.' <https://www.amnesty.org/download/Documents/EUR0125112020ENGLISH.PDF> accessed 6 August 2020.

issued during lockdown for violating regulations tripled the rest of the nation, despite assurances from authorities that lockdown measures were uniform throughout the country. [24]

Increases in the stated cases of police brutality within Europe, associated with COVID control enforcement have been noted:

> Romani communities in Slovakia reported numerous cases of police brutality, some against children playing outside. Black, brown and working-class communities across Europe are experiencing the physical and psychological effects of being watched even more than normal. In Brussels, where EDRi is based, a young man has died in contact with the police during raids.[25]

In Russia, Moscow officials ordered numerous police raids of hotels, apartments, and dormitories to track down Chinese people in the city. They were authorised to use facial recognition technology for tracking those who were suspected of evading the self-quarantine period upon their arrival. Identification technology were installed on public transportation like busses, underground trains and street trams. These efforts were coupled with transport workers being instructed to stop riders from China, essentially tracking and limiting their range of movement and association in efforts to contain the virus.[26] Discrimination via public transport will have exponential effect on poorer residents who have no other means for movement. The drivers in turn sought assistance from the Public Transport Workers Union being unsure of the protocols for identifying travellers on the basis of nationality. Union chairman Yuri Dashkov responded, "How can [a driver] ascertain that he saw a Chinese national, or a Vietnamese national, or a Japanese?"[27]

The escalation of targeted discrimination has prompted criticisms of inadequate and insufficient measures to ensure the safety of the vulnerable. In Italy, a non-governmental organisation, Avvocato di Strada, drafted a letter to state authorities calling for urgent anti-discrimination policies, stressing that authorities should not unduly sanction homeless people living on the streets given their inability to comply with lockdown measures.[28] Similarly, the United Nations Network on Migration has also called on authorities to take additional steps to mitigate xenophobia, recognising that migrants face greater obstacles to healthcare in large part due to language and cultural barriers. The UN further emphasised that access to treatment, care, and containment measures must be equitable for all since the only way overcome the pandemic is by ensuring adequate healthcare for everyone, regardless of their nationality or citizenship status.[29]

---

[24] 'Europe: COVID-19 Lockdowns Expose Racial Bias and Discrimination within Police' <https://www.amnesty.org/en/latest/news/2020/06/europe-covid19-lockdowns-expose-racial-bias-and-discrimination-within-police/> accessed 6 August 2020.
[25] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[26] The Associated Press and 2020 9:31 AM ET | Last Updated:, 'Moscow Targets Chinese with Raids amid Coronavirus Fears | CBC News' (*CBC*, 23 February 2020) <https://www.cbc.ca/news/world/coronavirus-russia-china-1.5473035> accessed 6 August 2020.
[27] The Associated Press and 2020 9:31 AM ET | Last Updated:, 'Moscow Targets Chinese with Raids amid Coronavirus Fears | CBC News' (*CBC*, 23 February 2020) <https://www.cbc.ca/news/world/coronavirus-russia-china-1.5473035> accessed 6 August 2020.
[28] 'Policing the Pandemic - Human Rights Violations in the Enforcement of COVID-19 Measures in Europe.' (n 23).
[29] 'OHCHR | COVID-19 Does Not Discriminate; nor Should Our Response' <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25730> accessed 17 August 2020.

It is evident that discrimination, while sectoral and sometimes rampant during the crisis, is contextual specific. Governments and individuals may seek to target already vulnerable groups in attempt to reinforce xenophobic differentiation into the social chaos caused by the pandemic, resulting in even greater social biases and worsening discriminatory practices. ***[Disquiet paper]***

~

During previous public health crises, people with diseases and their families have often faced discrimination and stigma.[30] For instance, people living with HIV in Kenya, South Africa, the Philippines, and the United States faced discrimination due to their HIV status and have been prevented from accessing health care, getting jobs, and attending school.[31] Likewise, the stigma against survivors of Ebola in West Africa, in some cases, had led to eviction, loss of employment, abandonment, violence, and other consequences.[32] 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.[33]

South Korean authorities believe that 63 percent of the 7,300 confirmed cases in the country as at 7 March 2020[34] attended services held by the Shincheonji Church of Jesus in the city of Daegu or had contact with attendees.[35] In a statement, the church reported 4,000 incidents against congregants since the outbreak, including termination of employment, workplace bullying, domestic persecution, and labelling, and the church was blamed as the leading reason of the COVID-19 outbreak.[36] Moreover, public health alerts around the virus may not have

[30] '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.
[31] 'Human Rights Dimensions of COVID-19 Response' (n 30).
[32] Luc Overholt and others, 'Stigma and Ebola Survivorship in Liberia: Results from a Longitudinal Cohort Study' (2018) 13 PLoS ONE <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6261413/> accessed 5 January 2021; J Daniel Kelly and others, 'Ebola Virus Disease-Related Stigma among Survivors Declined in Liberia over an 18-Month, Post-Outbreak Period: An Observational Cohort Study' (2019) 13 PLoS neglected tropical diseases e0007185.
[33] Incidents include physical attacks and beatings, violent bullying in schools, angry threats, discrimination at school or in workplaces, and the use of derogatory language in news reports and on social media platforms, among others. Since January, media have reported alarming incidents of hate crimes in the United Kingdom, the US, Spain, and Italy, among other countries, targeting people of Asian descent, apparently linked to COVID-19. Quentin Fottrell, '"No Chinese Allowed": Racism and Fear Are Now Spreading along with the Coronavirus' *MarketWatch* (3 February 2020) <https://www.marketwatch.com/story/no-chinese-allowed-racism-and-fear-are-now-spreading-along-with-the-coronavirus-2020-01-29> accessed 6 April 2020; Hwee Min Ang, '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.
[34] 'The Updates on COVID-19 in Korea as of 7 March' (*Korea Disease Control and Prevention Agency*, 7 March 2020) <https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030&act=view&list_no=366485&tag=&nPage=1> accessed 27 April 2020.
[35] 'Human Rights Dimensions of COVID-19 Response' (n 30).
[36] Raphael Rashid, 'Being Called a Cult Is One Thing, Being Blamed for an Epidemic Is Quite Another' *The New York Times* (9 March 2020) <https://www.nytimes.com/2020/03/09/opinion/coronavirus-south-korea-church.html> accessed 27 April 2020.

adequately protected the privacy of individuals with the virus.[37] Some tracing programmes have even led to the discovery of extramarital affairs.[38] [***Ethics paper***]

~

In 'Rule of Law in Times of Health Crises' the authors take time to engage the relevance of anti-discrimination for rule of law. They observe that the virus exposes existing inequalities and vulnerabilities in society. The different responses to COVID impact different communities in different ways and tend to exacerbate endemic social dysfunction such as domestic violence, as well as triggering social discriminators that disadvantage health care access for ethnic minorities. The report advocates that such discrimination must be addressed through positive policy action measures, in line with obligations under equality legislation and constitutional protections ensuring gender justice and racial harmony.

In the report's view, consideration must also be given to groups such as prisoners, persons in residential care, persons who are homeless and/or living in shelters, refugee settlements, along with certain categories of workers, that because of their living conditions are not able to benefit from social distancing or other less intrusive control measures. When it comes to frontline health care workers, many of whom in economically advanced countries are migrant workers, the inadequate or delayed supply of personal protective equipment also heightens the risk from vulnerability through exposure. ***[ROL paper]***

~

In this pandemic, we observe discrimination along the lines of income, occupation, socioeconomic status, ethnicity, race, nationality, gender, housing situation, and more.[39] African people in China are perceived as more infectious.[40] 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.[41] 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

[37] 'Coronavirus Privacy: Are South Korea's Alerts Too Revealing?' *BBC News* (5 March 2020) <https://www.bbc.com/news/world-asia-51733145> accessed 6 April 2020.
[38] One recent alert concerned a woman, aged 27, who works at the Samsung plant in Gumi. It said that at 11:30 at night on 18 February she visited her friend, who had attended the gathering of religious sect Shincheonji, the single biggest source of infections in the country. 'Coronavirus Privacy: Are South Korea's Alerts Too Revealing?' (n 37).
[39] 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.
[40] 'China: Covid-19 Discrimination Against Africans' (*Human Rights Watch*, 5 May 2020) <https://www.hrw.org/news/2020/05/05/china-covid-19-discrimination-against-africans> accessed 20 May 2020.
[41] 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.

to take as a given) regulatory interventions can and should minimise both forms of discrimination.

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 [be] 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.[42]

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.[43]
2. *Sometimes, we miscategorise similar people***.** For example, in many countries Chinese people, Africans or Hispanics are more likely to get categorised as "infectious".[44] 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 casual employment.[45] 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

[42] Kolitha Wickramage and others, 'Missing: Where Are the Migrants in Pandemic Influenza Preparedness Plans?' (2018) 20 Health and Human Rights 251; 'Note on the Protection of Migrants in the Face of the Covid-19 Pandemic' <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.

[43] Mari Yamaguchi, 'In Japan, Pandemic Brings Outbreaks of Bullying, Ostracism' *AP NEWS* (11 May 2020) <https://apnews.com/article/b666b40a92f26c352093494e47eeda6c> accessed 6 January 2021.

[44] Sherita Hill Golden, 'Coronavirus in African Americans and Other People of Color' (*Johns Hopkins Medicine*, 20 April 2020) <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.

[45] 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.

illuminated when we lump everybody into the social distancing imperative, and as such expect everyone is equally protected. ***[Covid Regulation paper]***

Infringement of human dignity as a result of discrimination

Human dignity is a leading principle in public health ethics.[46] 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.[47] 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.[48]

Discrimination based on presumed spread of the virus may have serious consequences for human dignity.[49] Respect for the integrity of one's personal data is indeed an integral part of 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. (...)

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. (...)

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. ***[Covid Regulation paper]***

~

Surveillance disproportionately affects data subjects across societies, depending on their situational vulnerability (such as residential status and occupational exposure) in terms of

[46] 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' (2018) 7 International Journal of Health Policy and Management 210.
[47] 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' (2015) 24 Information & Communications Technology Law 262.
[48] 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. Fottrell (n 33); Ang (n 33).
[49] Ryan Thoreson, 'Covid-19 Backlash Targets LGBT People in South Korea' *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.

liberties and personal data protection. A vocal source of disquiet stems from the employment sector, where different classes/strata of workers worry about possible adverse consequences for employment security posed by citizen surveillance. The abovementioned IPS study revealed that self-employed Singaporeans and part-time workers feared that the additional surveillance and monitoring, especially cell phone data tracking, could affect their livelihoods.[50] On the other hand, full-time employees, as well as those who experienced jobs losses because of the pandemic, were more likely to support the use of surveillance as they were anxious that without it, contact tracing efforts would be retarded, derailing any return to former work routines, and associated threats to job continuation.[51] Focused on the prospect of being able resume a previous work-life routine, these respondents were willing to accept interim privacy invasions and constraints on civil liberties, without according much weight to the potential impacts that such surveillance may have on other features of the quality of life.[52] ***[Disquiet paper]***

Bias and databases producing bias datasets

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. (...)

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.[53]

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.[54] This limitation could lead to people of colour being wrongly identified as potential carriers. ***[Covid Regulation paper]***

3.2 Interference with data protection regimes and privacy rights

The pandemic has also produced other deleterious outcomes to existing data protection regimes and personal privacy. This includes challenges posed to the integrity and security of one's personal data as a result of state surveillance (and data collection methods)

[50] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' <https://lkyspp.nus.edu.sg/docs/default-source/ips/ips-report-on-attitudes-towards-the-use-of-surveillance-technologies-in-the-fight-against-covid-19-240520.pdf> accessed 28 July 2020.
[51] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' (n 50).
[52] 'How Governments Can Build Trust in AI While Fighting COVID-19' (*World Economic Forum*) <https://www.weforum.org/agenda/2020/04/governments-must-build-trust-in-ai-to-fight-covid-19-here-s-how-they-can-do-it/> accessed 30 July 2020.
[53] Louise Matsakis, 'Scraping the Web Is a Powerful Tool. Clearview AI Abused It' [2020] *WIRED* <https://www.wired.com/story/clearview-ai-scraping-web/> accessed 5 January 2021.
[54] Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (2018) Proceedings of Machine Learning Research Conference on fairness, accountability and transparency 1.

including the potential harm directed at individual privacy rights, and the threat to individual anonymity as a result of data aggregation.

First, because pandemic containment measures are heavily dependent on the extraction and collection of personal data, its proper safekeeping, usage and ultimate destruction (when the public health threat ceases) must be closely monitored to ensure that data integrity and security is retained. Data subjects need also be kept in the loop to ensure that they are able to determine the location and appropriate/fair use of their personal private information. CAIDG's research has however revealed that citizens are not only uninformed but are anxious because of the apparent lack of information and updates from state authorities. Relatedly, as a result of COVID surveillance methods, state bodies continue to compromise on individuals' right to privacy leading to the slow erosion of this fundamental human right. Second, aggregated databases combining multiple data sources pose a threat to individuals' right to privacy, which may have a negative influence on their overall safety and security. Re-identification of anonymized data as a result of data aggregation may worsen bias, stigma and, discrimination against already marginalised groups.

Challenges to privacy rights and the integrity of one's personal data

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.[55] (...)

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 processors may run contrary to any of the data sharing practices that have emerged during the COVID-19 containment crisis. ***[Covid Regulation paper]***

~

Regarding efficiency and necessity, our survey reveals there has been inadequate public, detailed and balanced justifications explained throughout effected communities concerning how vast data collection, and mass sharing of such data will be appropriately utilised to impede the spread of the virus, as well as how long the data will be retained, and by whom. This dearth of explanatory engagement in many surveillance settings is accompanied by insufficient commitment from sponsoring agencies to identify and explain the limitations of control purpose achievement and the compromises required from civil society to better ensure control outcomes.[56]

By exploring community concerns regarding the use of AI-assisted surveillance technology in pandemic control responses, regulators will be better placed to evaluate risk and benefit in

[55] Mark Findlay and others, 'Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-Emptive Tracing Post-Crisis' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3592283 <https://papers.ssrn.com/abstract=3592283> accessed 4 August 2020.

[56] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (*EDRi*, 27 May 2020) <https://edri.org/surveillance-is-a-pre-existing-condition/> accessed 21 July 2020.

terms of identified health and safety outcomes, against challenges to liberties, personal data integrity and citizens' rights, rather than simply retiring into the assertion of necessary trade-offs. If policy planners deem a technology essential and explain this in detail to their data subjects, consideration of in-built regulatory mechanisms for ethical compliance feature can and will more prominently in operational roll outs.[57] (...)

Pandemic control data collection extends beyond contact tracing apps into more invasive forms of tracing measures, including: surveillance monitoring technology such as CCTVs, electronic tagging wristbands, temperature sensors, drones, etc. A common and prevailing anxiety voiced by citizens across states and communities surveyed centres on key questions of data integrity and personal protection - *what forms* of data are being stored, whether the mass amounts of data collected are stored appropriately,[58] who can *use and own* the data collected,[59] and for *how long* the data will be retained? (...)

[...] approval for mass data use and sharing, particularly during the pandemic, is dependent on numerous factors including: the nature of the data in question; the extent to which individual data subjects are convinced of its integrity and security; and the availability of information pathways for individuals to seek adequate explanations of how their data is being collected, used, and stored. (...)

[...] the centralisation of data within a state-controlled repository for Australia's COVIDSafe[60] app also drew speculation about potential data breaches since mass volumes of data are being stored only in a single government database.[61] The reliability and safety of data collected have been critically discussed, while fears are exacerbated by a lack of information regarding what safeguards are put in place to ensure that the collected data would not be prone to misuse.[62] Such reservations about government probity materialise in instances where authorities allegedly illegally accessed metadata searches (over 100 times) and falsified warrants to target media journalists.[63] (...)

---

[57] Mark Findlay and Nydia Remolina, 'Regulating Personal Data Usage in COVID-19 Control Conditions' (2020) No. 2020/04 SMU Centre for AI & Data Governance <https://papers.ssrn.com/abstract=3607706> accessed 20 July 2020.

[58] Arjun Kharpal, 'Use of Surveillance to Fight Coronavirus Raises Concerns about Government Power after Pandemic Ends' (*CNBC*, 26 March 2020) <https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html> accessed 20 July 2020.

[59] Genevieve Bell, '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.

[60] On 14 April 2020, the Australian Government announced the development of a contact tracing app that was subsequently launched on 26 April 2020. See: 'The Government Wants to Track Us via Our Phones. And If Enough of Us Agree, Coronavirus Restrictions Could Ease' (14 April 2020) <https://www.abc.net.au/news/2020-04-14/coronavirus-app-government-wants-australians-to-download/12148210> accessed 1 September 2020; 'The Coronavirus Tracing App Has Been Released. Here's What It Looks like and What It Wants to Do' (26 April 2020) <https://www.abc.net.au/news/2020-04-26/coronavirus-tracing-app-covidsafe-australia-covid-19-data/12186068> accessed 1 September 2020.

[61] Tamar Sharon, 'Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers' [2020] Ethics and Information Technology 1.

[62] 'Is AI Trustworthy Enough to Help Us Fight COVID-19?' (*World Economic Forum*) <https://www.weforum.org/agenda/2020/05/covid19-coronavirus-artificial-intelligence-ai-response/> accessed 27 July 2020.

[63] 'Police Made Illegal Metadata Searches and Obtained Invalid Warrants Targeting Journalists' (*the Guardian*, 23 July 2019) <http://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists> accessed 5 August 2020.

In a recent study conducted by the Institute of Policy Studies (IPS) on respondents in Singapore, those surveyed expressed a willingness to sacrifice their privacy to a degree, in order to resume their daily activities as soon as possible.[64] Slightly under half of the respondents were agreed to having their phone data tracked without their consent, for contact tracing purposes. IPS indicated that around 60% of the respondents believed TraceTogether, or a similar contact tracing phone app, should be made mandatory to download and its use compulsory for entry to public spaces, suggesting that Singaporeans are generally supportive of the government's efforts in handling the pandemic in terms of specific response technologies.[65] Recognising the responsibility which should attach to such significant levels of public support, IPS warned that any ongoing forms of large-scale government-sanctioned surveillance programmes will inevitably raise questions about data protection and individual liberties that must be addressed by government and other data sharers, (i.e., how sensitive personal data will be used, who has its access, and whether private companies will be allowed to utilise and exploit it in the future for commercial, non-pandemic related purposes).[66] (...)

It is unclear to data subjects in many of the contexts reviewed what types of data are being collected and what its intended use is for. This is especially true for non-health information (e.g. financial transaction information via credit cards) being collected and analysed by state agencies during health crises.[67]

Disquiet concerning the invasion of rights and liberties appears to be dependent on the nature of the 'rights' under challenge, who poses the challenge, and associated specific community sensitivity about data content. A recent survey looking to position Singapore's approach to surveillance control compared with other jurisdictions discovered that if personal medical data was exposed through surveillance, then acceptance of its dissemination was heavily dependent on whether it would be seen and used by personal medical practitioners, or by public health officials, rather than government officials at large. In addition, the same survey interestingly noted:[68]

> Half of Singaporeans would also be comfortable sharing location data from mobile telephones as part of an effort to trace potential contact with infected persons, with other surveyed countries beside Spain returning much lower consent rates. As noted by Oliver Wyman, China and South Korea, which both managed to sharply reduce the rates of community infection following their respective outbreaks, have used such mobile location tracking in their containment efforts.
>
> "Most people support sharing personal health data if it's aimed at protecting their health and that of the wider public," concludes the Oliver Wyman survey-report. "They are much less interested in doing so to obtain cheaper or more convenient health care, or other goods and services. They also are less willing to share non-health information,

[64] 'Singaporeans Accept Some Privacy Loss in Covid-19 Battle but Surveillance Method Matters: IPS Study' (*The Straits Times*, 25 May 2020) <https://www.straitstimes.com/singapore/singaporeans-accept-some-privacy-loss-in-covid-19-battle-but-surveillance-method-matters> accessed 22 July 2020.
[65] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' (n 50).
[66] 'Singaporeans Accept Some Privacy Loss in Covid-19 Battle but Surveillance Method Matters: IPS Study' (n 64).
[67] 'How Governments Can Build Trust in AI While Fighting COVID-19' (n 52).
[68] 'Singaporean Attitudes to Personal COVID Data Differ to Overseas Counterparts' (*Consultancy.asia*, 15 April 2020) <https://www.consultancy.asia/news/3126/singaporean-attitudes-to-personal-covid-data-differ-to-overseas-counterparts> accessed 20 July 2020.

such as mobile phone location or financial transaction data, even if it's used to track potential contact with infected persons. (...)

South Korean officials have emphasised that any privacy infringements resulting from surveillance technology must be weighed against "disastrous economic consequences from a long-term shutdown".[69] In keeping with the economic consequences justifying intrusive and sometimes selective surveillance and data analysis, Ministries concede that banning free movement during a crisis is a problematic restriction of freedom.[70] However, whether or not states translate this awareness into firm policy qualifiers for reducing emergency surveillance measures remains to be seen. ***[Disquiet paper]***

~

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.[71] ***[Covid Regulation paper]***

~

As the COVID-19 health pandemic rages governments and private companies across the globe are utilising AI-assisted[72] surveillance, reporting, mapping and tracing technologies with the intention of slowing the spread of the virus. These technologies have capacity to amass personal data and share data sources for community control and citizen safety motivations that empower state agencies and persuade citizen co-operation which could only be imagined outside such times of real and present danger. Concern is growing about the potential for these technologies and resultant data sharing to negatively impact civil rights,[73] invade personal privacy,[74] undermine citizen dignity through expansive data matching and provide opportunities for data use well beyond the brief of virus mitigation.[75] (...)

The COVID-19 situation is not the first health crisis where public safety reasons were advanced to restrict individual rights, especially related to data protection and the responsible use of data.

---

[69] 'Cyber-Intel Firms Pitch Governments on Spy Tools to Trace Coronavirus' (*CNBC*, 28 April 2020) <https://www.cnbc.com/2020/04/28/cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus.html> accessed 21 July 2020.

[70] 'Cyber-Intel Firms Pitch Governments on Spy Tools to Trace Coronavirus' (n 69).

[71] 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; Findlay and others, 'Ethics, AI, Mass Data and Pandemic Challenges' (n 55).

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

[73] 'Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights' <https://www.amnesty.org/download/Documents/POL3020812020ENGLISH.pdf> accessed 6 April 2020.

[74] Albert Gidari, 'Op-Ed: How Location History Can Help Contain COVID-19 While Protecting Privacy - Risky Business' (*Risky.biz*, 27 March 2020) <https://risky.biz/gidarioped/> accessed 6 April 2020.

[75] Guariglia and Schwartz (n 71).

In 2014, privacy concerns urged the GSM Association[76] to issue guidelines on the protection of privacy in the use of mobile-phone data for responding to the Ebola outbreak.[77] In the present crisis similar concerns emerge about the secondary use of public health control data. There have been reports that China's digital epidemic control might have exacerbated stigmatisation and public mistrust.[78] (...)

[The excerpt below engages in a more specific discussion on whether the data procured through MOM monitoring complies with personal data protection guidelines in Singapore]

It should firstly be noted that the Personal Data Protection Act ("PDPA") generally does not apply to "any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data".[79] Consequently, the various obligations under the PDPA relating to consent, purpose limitation, notification, access and correction, accuracy, protection, retention limitation, transfer limitation, etc, do not apply to public agencies.

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

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

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

~

[76] An industry organization that represents the interests of mobile-network operators worldwide.
[77] 'GSMA Guidelines on the Protection of Privacy in the Use of Mobile Phone Data for Responding to the Ebola Outbreak' (*Groupe Speciale Mobile Association*, 19 November 2014) <https://www.gsma.com/mobilefordevelopment/resources/gsma-guidelines-on-the-protection-of-privacy-in-the-use-of-mobile-phone-data-for-responding-to-the-ebola-outbreak/> accessed 27 April 2020.
[78] Marcello Ienca and Effy Vayena, 'On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic' (2020) 26 Nature Medicine 463.
[79] s4(1)(c) of the 'Personal Data Protection Act 2012 - Singapore Statutes Online' <https://sso.agc.gov.sg/Act/PDPA2012> accessed 13 October 2020.

Data aggregation, reidentification and threat to anonymity

Gaining access to data from personal devices for contact tracing purposes, for example, can be justified if it occurs within specific bounds, has a clear purpose - e.g., warning and isolating people who may have been exposed to the virus - and other minimally invasive alternatives are not suitable —e.g., using anonymised mobile positioning data.[80]

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.[81]

Moreover, data aggregation is however 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.[82] 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)? ***[Covid Regulation paper]***

~

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

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,[83] or to play a part in containing the virus, counter-narratives have emerged which rehearse reservations about the consequences of such mass data sharing. Urs Gasser from Harvard Law School's Berkman Klein Centre casts doubt on the risks and benefits in mining data to combat COVID-19, and aggregated mobility data in particular.[84] Gasser not only identifies privacy concerns but more pragmatic fit-for-purpose considerations. The Oxford

[80] Ienca and Vayena (n 78).
[81] Kirsten E Martin, 'Ethical Issues in the Big Data Industry' (2015) 14 MIS Quarterly Executive 67.
[82] 'Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us out of Lockdown' (*University of Oxford*, 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.
[83] Cass R Sunstein, 'The Meaning of Masks' (2020) Forthcoming JOURNAL OF BEHAVIORAL ECONOMICS FOR POLICY <https://papers.ssrn.com/abstract=3571428> accessed 5 January 2021.
[84] Gasser Urs, 'How Much Access to Data Should 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/> accessed 27 April 2020.

Covid Impact Monitor[85] uses population movement data, provided by Cuebiq, which is a location intelligence and measurement platform. Through its Data for Good programme, Cuebiq offers access to aggregated and privacy-enhanced mobility data for academic research and humanitarian initiatives. They claim, "this first-party data is collected via anonymised users who have opted-in to provide access to their location data anonymously". Cuebiq basically shares their advertising tracking database governed by a privacy policy that pre-existed the COVID crisis and they have already been collaborating with partners in several "humanitarian" initiatives.[86] Oxford's website states: "Ethical big data can help save lives". However, there seems to be nothing on their website addressing ethical challenges beyond saying that they use anonymous data, which of itself does not address fairness issues or future misuses of data. ***[Ethics paper]***

~

The intrusiveness of community surveillance has drawn sustained criticisms from human rights groups and the public alike, particularly when assurances concerning de-identification have not been accepted. [...] an instance of the re-identification of patients' health data accompanied the 2016 health data breach in Australia, in spite of a prior de-identification of personal data to safeguard patients' privacy.[87]

Similarly in South Korea, the wide harvesting and sharing of data (originally implemented during the outbreak of Middle East Respiratory Syndrome (MERS) in 2015)[88] amassed from credit card transactions, phone geolocation, surveillance footage, facial scans, and temperature monitors were employed to enforce targeted lockdowns.[89] More recently, the detailed collection of highly personal details (via the abovementioned surveillance measures) regarding patients' whereabouts have enabled the re-identification of COVID-positive patients,[90] which is said to have resulted in the harassment and doxing of certain targeted individuals. In response, authorities have cut back on their data-sharing activities,[91] although this appears to be insufficient to adequately address existing infringements of privacy. Evidently, such reactionary measures would undoubtedly have limited impact on the massive data already collected, processed and shared.

Anonymity and the aggregation of data are constantly discussed amongst COVID control data subjects and privacy commentators. As Yves-Alexandre de Montjoye, head of the computational privacy group at Imperial College London shared, "[the] challenge with this data is that we don't believe it can be anonymized". This observation is premised on Montjoye's research, which made the discovery that almost all individuals could be personally identified

[85] 'Oxford COVID-19 Impact Monitor' (*University of Oxford*) <https://grapher.oxford-covid-19.com/grapher/gyration_2020-04-02> accessed 27 April 2020.
[86] For some examples see 'Data for Good' (*Cuebiq*) <https://www.cuebiq.com/about/data-for-good/> accessed 27 April 2020.
[87] Dr Vanessa Teague Melbourne, 'The Simple Process of Re-Identifying Patients in Public Health Records' (*Pursuit*, 18 December 2017) <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records> accessed 5 August 2020.
[88] 'Privacy vs. Pandemic Control in South Korea' (*The National Law Review*) <https://www.natlawreview.com/article/privacy-vs-pandemic-control-south-korea> accessed 5 August 2020.
[89] 'How Governments Can Build Trust in AI While Fighting COVID-19' (n 52).
[90] 'Ensuring Data Privacy as We Battle COVID-19' (*OECD*) <https://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/> accessed 4 August 2020.
[91] Mary Ilyushina CNN, 'How Russia Is Using Authoritarian Tech to Curb Coronavirus' (*CNN*) <https://www.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html> accessed 30 July 2020.

from just four pieces of anonymised mobile phone data. While companies and governments strenuously assert that data can be anonymised to protect individuals' identities and privacy,[92] contesting findings by critical commentators may generate confusion and wariness about the extent to which their privacy is protected through the declared anonymisation of data. Along with these suspicions, data subjects become increasingly circumspect about the kinds of data sharing activities between public and private institutions deploying intrusive surveillance strategies, when data amassed from recognition technology has the specific intention of identifying individuals.[93] ***[Disquiet paper]***

3.3 Risk of surveillance creep and anxiety governance

The push for data capture and the increase of COVID-19 surveillance infrastructures has also led to concerns of the risk of surveillance creep. Activists and scholars have cautioned that States may be reluctant to relinquish or phase out intrusive surveillance techniques/technologies even after the health crisis subsides. This carries serious consequences for individual privacy and liberty rights. There is also a looming threat that States may engage with surveillance data (that may be biased, unrepresentative or unobjective) for other social ordering or engineering purposes.

Citizens' unwavering and unquestioning compliance to State's pandemic containment measures must also be scrutinised. Data subjects ought to be cognizant that these unusual measures may be normalised into the future as States take advantage of citizens' anxieties to deny and diminish protection of individual rights and liberties.

Surveillance Creep

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.[94] (...)

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

[92] '9 Geeky Myth-Busting Facts You Need to Know about TraceTogether' <https://www.tech.gov.sg/media/technews/geeky-myth-busting-facts-you-need-to-know-about-tracetogether> accessed 4 August 2020; Josh Taylor, 'Covidsafe App: How Australia's Coronavirus Contact Tracing App Works, What It Does, Downloads and Problems' *The Guardian* (15 May 2020) <https://www.theguardian.com/australia-news/2020/may/15/covid-safe-app-australia-how-download-does-it-work-australian-government-covidsafe-covid19-tracking-downloads> accessed 4 August 2020.

[93] Stephanie Findlay, Richard Milne and Stefania Palma, 'Coronavirus Contact-Tracing Apps Struggle to Make an Impact' (18 May 2020) <https://www.ft.com/content/21e438a6-32f2-43b9-b843-61b819a427aa> accessed 4 August 2020.

[94] Guariglia and Schwartz (n 71).

respiratory outbreaks that are seasonal, deadly, but do not advocate for such intrusive personal surveillance. (...)

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.[95] ***[Covid Regulation paper]***

~

Anxiety Governance and its impact

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.[96] 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.[97]

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 government has already been circulating mass 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[98] can make salient the public gains from mass adoption, thereby appealing to social norms and peer pressure in further encouraging app adoption.[99] Texts could also make people aware of the extent to which others in their community, or

[95] Mark Findlay and others, 'Ethics, AI, Mass Data and Pandemic Challenges: Responsible Data Use and Infrastructure Application for Surveillance and Pre-Emptive Tracing Post-Crisis' (2020) No. 2020/02 SMU Centre for AI & Data Governance Research Paper <https://papers.ssrn.com/abstract=3592283> accessed 6 January 2021.

[96] 'Mental Health and COVID-19' (*World Health Organisation*) <https://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/publications-and-technical-guidance/noncommunicable-diseases/mental-health-and-covid-19> accessed 29 April 2020.

[97] 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/article/4ayywp/refusing-to-use-coronavirus-contact-tracing-app> accessed 20 May 2020.

[98] Sunstein (n 83).

[99] David P Bryne, 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*, 27 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.

neighbouring communities, have downloaded the app, associated research suggesting that unfavourable social comparisons would motivate app adoption.[100] ***[Covid Regulation paper]***

~

Most recently, the Singapore government has announced a pilot programme combining the use of SafeEntry and TraceTogether data to improve the contact tracing process.[101] SafeEntry, an island-wide mandated digital check-in system that logs data subjects' visited locations, relies on location records.[102] On the other hand, the government has repeatedly emphasised that TraceTogether is privacy-centric, processing anonymised proximity data and not geolocation indicators to assist in contact tracing efforts.[103] Given the voluntary nature of TraceTogether, it was not necessary for data subjects to use both SafeEntry and TraceTogether, although they have been encouraged to do so. However, from October 2020, data subjects participating in larger events such as meetings, incentives, conferences and exhibitions (MICE) will be required to use only the TraceTogether app in order to log a SafeEntry check-in.[104] This conflation of technology and purpose appears to be a roundabout way to mandate the use of the originally voluntary TraceTogether app, while also suggesting that authorities will be using both location and proximity data to monitor data subjects – heightening the already intrusive capacity of control strategies. This move signals that Singapore is shifting towards mandating the use of TraceTogether, by ensuring that the TraceTogether technology (be it the app or the token) must be used when checking into major events as re-opening of the country progresses. This change in the conditions of citizen compliance may raise suspicions amongst its users and challenges citizen self-determination with regards to their app use and data sharing.[105] The lower-than-necessitated uptake of TraceTogether may lie behind this development but challenges to trust because of compulsory application will also diminish citizen cooperation. At the time of writing, the abovementioned concerns have been realised in a recent press briefing on 20 October 2020, where the multi-ministry task force tackling COVID-19 declared that TraceTogether will be made mandatory by December 2020.[106] In addition, by making a

[100] Per Engström and others, 'Tax Compliance and Loss Aversion' (2015) 7 American Economic Journal: Economic Policy 132.
[101] Linette Lai, 'Pilot to Require Check-Ins Using TraceTogether' (*The Straits Times*, 10 September 2020) <https://www.straitstimes.com/singapore/pilot-to-require-check-ins-using-tracetogether> accessed 10 September 2020.
[102] 'How Are My Possible Exposures Determined?' (*TraceTogether FAQs*) <http://support.tracetogether.gov.sg/hc/en-sg/articles/360053464873> accessed 10 September 2020.
[103] 'How Does the TraceTogether App Work?' (*TraceTogether FAQs*) <http://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473> accessed 11 September 2020.
[104] 'Media Release - TraceTogether and SafeEntry to Be Enhanced in Preparation for Further Opening of the Economy.Pdf' <https://www.sgpc.gov.sg/sgpcmedia/media_releases/sndgo/press_release/P-20200909-1/attachment/Media%20Release%20-%20TraceTogether%20and%20SafeEntry%20to%20be%20Enhanced%20in%20Preparation%20for%20Further%20Opening%20of%20the%20Economy.pdf> accessed 11 September 2020; 'Singapore Plans New Layer of Coronavirus Contact Tracing to Enable Larger Events' (*South China Morning Post*, 9 September 2020) <https://www.scmp.com/week-asia/health-environment/article/3100912/singapore-expand-use-tracetogether-it-opens-events-250> accessed 10 September 2020.
[105] 'Research/Policy Comment Series (1): Strengthening Measures for Safe Reopening of Activities: Ethical Ramifications and Governance Challenges | Centre for AI & Data Governance' <https://caidg.smu.edu.sg/strengthening-measures-safe-reopening-activities-ethical-ramifications-and-governance-challenges> accessed 1 October 2020.
[106] Lester Wong, 'Use of TraceTogether App or Token Mandatory by End Dec' (*The Straits Times*, 21 October 2020) <https://www.straitstimes.com/singapore/use-of-tracetogether-app-or-token-mandatory-by-end-dec> accessed 21 October 2020.

70% take-up rate of TraceTogether a condition for re-opening up the country,[107] this confirms the state's prioritization of more stringent surveillance rather than citizen self-determination. (...)

(…) to counter the slow uptake of contact tracing apps following inadequate clarifications and growing distrust, federal authorities mooted compulsory citizen subscription.[108] In an effort to deal with these and other public reservations, the Commonwealth government sought to introduce legislation stipulating mandatory privacy protection regimes to be imposed on COVID control tracking and surveillance applications.[109] Deputy Chief Medical Officer Paul Kelly announced that the government would "start with voluntary" downloads of COVIDSafe, to assess whether it was necessary to "[force] Australians to download" the app.[110] However, officials quickly back-peddled on mandatory downloads owing to public backlash against suggestions of political coercion.[111] In a tweet, Prime Minister Scott Morrison expressly stated that the app will "not be mandatory".[112] Nevertheless, stronger intrusive measures are already starting to surface, with military officers being deployed into urban areas in Australia to ensure citizens' strict adherence to quarantine and lockdown regulations.[113] More recently, Prime Minister Scott Morrison announced a possibility of mandating coronavirus immunisation for all 25 million Australians, a move that has sparked ethical and safety debates.[114]

In response, sections of the Australian public have sought to counter the government's control responses through nationwide protests (including Melbourne,[115] New South Wales,[116] and

[107] 'TraceTogether SafeEntry Token & App Must Be Used by 70% of S'pore Population to Enter Phase 3' <https://mothership.sg/2020/10/tracetogether-safeentry-token-70-percent/> accessed 21 October 2020.
[108] 'Coronavirus Mobile Tracking App May Be Mandatory If Not Enough People Sign up, Scott Morrison Says' (*SBS News*) <https://www.sbs.com.au/news/coronavirus-mobile-tracking-app-may-be-mandatory-if-not-enough-people-sign-up-scott-morrison-says> accessed 5 August 2020.
[109] The legislation is detailed in Graham Greenleaf and Katharine Kemp, Graham Greenleaf and Katharine Kemp, 'Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3601730> accessed 27 July 2020.
[110] 'Deputy CMO Doesn't Rule out Forcing Australians to Download Contact Tracing App' (17 April 2020) <https://www.abc.net.au/news/2020-04-17/paul-kelly-coronavirus-tracing-app/12158854> accessed 5 August 2020.
[111] '"No Geolocation, No Surveillance": Government Makes Privacy Assurances over Coronavirus App' (18 April 2020) <https://www.abc.net.au/news/2020-04-18/prime-minister-rules-out-making-coronavirus-app-mandatory/12161126> accessed 5 August 2020.
[112] 'Scott Morrison on Twitter: "The App We Are Working on to Help Our Health Workers Trace People Who Have Been in Contact with Coronavirus Will Not Be Mandatory." / Twitter' (*Twitter*) <https://twitter.com/ScottMorrisonMP/status/1251304490952605696> accessed 5 August 2020.
[113] 'Australia's Victoria State to Deploy Military, Impose A$5,000 Fines to Enforce Coronavirus Isolation' (*The Straits Times*, 4 August 2020) <https://www.straitstimes.com/asia/australianz/australias-victoria-state-to-impose-fines-of-almost-a5000-for-breaching-covid-19> accessed 5 August 2020.
[114] 'Coronavirus Vaccine Should Be Mandatory, Says Australia PM as Race Heats Up' (*The Straits Times*, 19 August 2020) <https://www.straitstimes.com/asia/australianz/coronavirus-vaccine-should-be-mandatory-in-australia-pm-morrison> accessed 20 August 2020.
[115] 'Coronavirus: Arrests at Australia Anti-Lockdown Protests' *BBC News* (5 September 2020) <https://www.bbc.com/news/world-australia-54040278> accessed 8 September 2020; Zach Hope Dexter, '"It Won't Stop": Anti-Lockdown Protesters Buoyed by Saturday Turnout' (*The Age*, 5 September 2020) <https://www.theage.com.au/national/victoria/heavy-police-force-greets-anti-lockdown-protesters-across-melbourne-at-the-shrine-20200905-p55so3.html> accessed 8 September 2020.
[116] 'Six "anti-Lockdown Protesters" Charged over NSW "Freedom Day" Rallies' <https://www.9news.com.au/national/coronavirus-sydney-anti-lockdown-protests-police-charges-melbourne-victoria-freedom-day-rallies-covid19/1df4547a-f4f4-4284-acd4-808432532eec> accessed 8 September 2020.

more specifically Sydney[117]) against lockdown measures. Hundreds of anti-lockdown protestors gathered together during "Freedom Day" rallies, chanting "freedom" and "human rights matter",[118] opposing restrictions of personal movement and association. Some of the protests held turned violent, which led to arrests of citizens in Sydney and Byron Bay.[119] ***[Disquiet paper]***

~

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. ***[Ethics paper]***

3.4 The threat to democracy and State legitimacy

The excerpts below show how State legitimacy and democracy has been threatened as a result of disproportionate and invasive pandemic-handling strategies. This challenge may arise as a result of a misuse or abuse of powers (by authoritative persons) in crisis handling, concentration of powers in the executive, the bypassing of parliament in the enactment of COVID-related laws, the use of emergency powers that are extended ad infinitum with no authoritative basis, or infringements and non-adherence to the rule of law. These factors have an influence on citizens' trust and confidence in the State. Notably, negative trust outcomes and compromised State legitimacy would interfere with the overall effectiveness of pandemic containment responses and the ultimate eradication of the virus.

Particular challenges to rule of law posed by pandemic responses including:

- Collection and processing of personal data
- Target surveillance (enforced quarantines and movement tracing)
- Strategic surveillance (such as QR code registration on entry)
- Video surveillance (CCTV cameras, facial recognition at ports of entry)
- Sensor surveillance (residential monitoring) ***[ROL paper]***

~

[117] 'Arrests Made at Anti-COVID-19 Protests in Sydney' (4 September 2020) <https://www.abc.net.au/news/2020-09-05/covid-19-protests-across-sydney-spark-arrests/12632660> accessed 11 September 2020.
[118] 'Arrests Made at Anti-COVID-19 Protests in Sydney' (n 117); 'Coronavirus: Arrests at Australia Anti-Lockdown Protests' *BBC News* (5 September 2020) <https://www.bbc.com/news/world-australia-54040278> accessed 8 September 2020.
[119] 'Coronavirus: Arrests at Australia Anti-Lockdown Protests' (n 118).

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. (...)

Many of the measures implemented by governments are based on extraordinary powers, only to be used temporarily in emergencies that allow government to disregard to some extent certain applicable laws, such as privacy protection provisions. In other instances, legal authority rests on permanent infectious diseases legislation but these are only to be activated in crisis contexts.[120] Some forms of authority, for instance, use exemptions in data protection laws to share data.[121] Most of these measures claim to be temporary, necessary, and proportionate. However, largely they have not addressed ethical issues so far.[122] ***[Covid Regulation paper]***

~

The connection between distrust and failed utility [123]

(...) we have sought to demonstrate that the lack of transparency surrounding the use of AI-assisted technology, coupled with inconsistent authoritative control responses, has resulted in public disquiet as data subjects experience frustration and doubt regarding the technology and the legitimacy of the state, in its control applications. For instance, with contact tracing apps presently operating on a by-consent model, the disengagement of the public from these technologies has grown out of, and perpetuated, distrust which inevitably resulted in a de-incentivization of app use. Consequently, reduced participation in consent-based technology has limited the prevention and control objectives of the digital tracing measures to curb the spread of the pandemic.

Despite similar digital contract tracing processes and technologies being implemented across different jurisdictions, the nature and extent of distrust appears to be context specific. In Singapore, despite the compulsory requirement of SafeEntry QR codes[124] enabling citizens to

---

[120] 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.

[121] 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 Yeon-Ji Kim, '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) <http://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* (6 March 2020) <http://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives> accessed 27 April 2020.

[122] Findlay and others, 'Ethics, AI, Mass Data and Pandemic Challenges' (n 95).

[123] Header from original paper.

[124] Since 6th July 2020, data subjects can use the TraceTogether app to scan SafeEntry QR codes. 'SafeEntry - National Digital Check-in System' <https://safeentry.gov.sg/> accessed 31 August 2020.

check-in and out of venues,[125] this technology has generated less disquiet compared to the voluntary TraceTogether app. Despite the nation-wide mandated implementation of SafeEntry within areas like shopping malls and office buildings, data subjects may perceive greater agency in their ability to control their interactions with the technology (e.g. when they *choose* to visit malls, markets, etc.), in contrast to TraceTogether which constantly runs in the background of users' phones.[126] In this instance, data subjects are more open to use the SafeEntry app with relatively less resistance, which has permitted more efficient tracing through this medium.[127] The capacity for citizens to choose whether they will or will not activate the app for entry gives a sense of self determination, and the data subjects feel more in touch with the purpose of the technology and the data it produces, even if in fact both TraceTogether and SafeEntry source data back to a centralised state storage an analysis facility. The perception of self-determination, which looks to be important in reducing disquiet and resistance may in fact be illusory when talking about entry into essential services. Even so it appears influential in favouring the technology.

In comparison, when a similar QR Code application, ProteGO Safe, was announced in Poland, the app garnered negative feedback. An initial proposal consisted of relying on QR Codes to manage the number of customers entering and exiting shopping malls. These restrictive purposes raised questions about the equitable voluntary nature of the app's coverage and the extent to which it impeded citizens to move freely. The app seemed not to facilitate entry but to qualify who could or could not gain admission, and as such self-determination was moderated by the app's accommodation capacity determinants. ProteGO Safe's development team subsequently admitted that they were unaware of such concerns, which prompted officials to abandon the QR code facility, labelling this incident as a "communication glitch".[128] In efforts to address this disquiet, Poland adapted ProteGO Safe to "secure privacy issues" by using anonymous keys based on Apple-Google's framework (over its initial Bluetooth logging technology) hoping to persuade greater uptake of the app.[129] However, poor app reviews[130] and surging numbers of infections[131] suggest that data subjects remain unsure about digital tracing technologies which could have a positive impact in hindering the spread of the virus.

---

[125] 'Things to Know about Singapore's Contact Tracing System SafeEntry' (*Time Out Singapore*) <https://www.timeout.com/singapore/news/things-you-might-not-know-about-singapores-digital-check-in-system-safeentry-051120> accessed 31 August 2020.

[126] We caveat that this understanding of choice is nominal, especially when data subjects must use these apps in premises like schools and work buildings. See: 'Research/Policy Comment Series (1): Strengthening Measures for Safe Reopening of Activities: Ethical Ramifications and Governance Challenges | Centre for AI & Data Governance' (n 105).

[127] Cara Wong, 'Digital Tools Help Speed up Contact Tracing Efforts to Ring-Fence Covid-19 Cases' (*The Straits Times*, 8 July 2020) <https://www.straitstimes.com/singapore/digital-tools-help-speed-up-contact-tracing-efforts-to-ring-fence-cases> accessed 2 September 2020.

[128] Deutsche Welle (www.dw.com), 'Coronavirus Contact Tracing Reignites Polish Privacy Debate | DW | 30.05.2020' (*DW.COM*) <https://www.dw.com/en/coronavirus-contact-tracing-reignites-polish-privacy-debate/a-53600913> accessed 31 August 2020.

[129] 'Poland Rolls out Privacy-Secure Coronavirus Tracking App' (*CNA*) <https://www.channelnewsasia.com/news/business/poland-rolls-out-privacy-secure-coronavirus-tracking-app-12820298> accessed 2 September 2020.

[130] As of 2 September 2020, Google Play recorded a 2.4 star review of the ProteGO Safe app. 'ProteGO Safe - Apps on Google Play' <https://play.google.com/store/apps/details?id=pl.gov.mc.protegosafe&hl=en> accessed 2 September 2020.

[131] 'Number of Confirmed Coronavirus Cases in Poland Reaches 67,922' <https://www.thefirstnews.com/article/number-of-confirmed-coronavirus-cases-in-poland-reaches-67922-15347> accessed 2 September 2020.

Accepting that distrust is common in contexts of disquiet, and the nature of disquiet and resistance are context specific, it is also unsurprising that positive citizen association with these apps and greater subscription, allows governments to accomplish their prevention and control goals for the tracing apps. Alternatively, if negative perceptions are not properly, promptly and personally addressed, governments will struggle against an anti-participation culture, leading to dissatisfaction with the performance of the tech, increased unhappiness with surveillance, and even protests and petitions against government responses that require a compromise of liberties and personal data protection.[132] This will potentially become a vicious cycle – apps are distrusted, their efficacy is impeded through lower uptake, virus control outcomes are negative and the citizen loses faith in the state's capacity to control the pandemic.

Paradoxically, the only justification in the eyes of citizens for technological surveillance of this type is its capacity to contain the pandemic. Because data subjects doubt this efficacy or are unwilling to achieve it at a cost to their independence and integrity, the failure of the applications is further fuel for disaffection. The problem appears to lie with a problematic argument that pandemic control can only be achieved when civil liberties and data integrity are compromised. Citizens do not accept such trade-offs in many situations detailed in the earlier sections of this paper. (...)

From the nature and dynamics of disquiet reviewed so far, it seems inevitable that trust must be as important a consideration in the development of pandemic control policy as are efficacy, robustness and adaptability. In addition, we have seen insufficient evidence that employing principled design from the outset of pandemic response technology development will reduce efficacy. In fact, the evidence points the other way. Principled design will improve trust. Along with trust comes effective capacity. (...) [***Disquiet Paper***]

3.5 Tech-related challenges

This section explores the specific challenges that have arisen as a result of the adoption of COVID control technologies in this pandemic. These technologies may produce negative social outcomes as a result of deficiencies in the inherent architecture (design) or operation/application of the technologies employed. This may be the result of States neglecting AI ethics and principled design (e.g., transparency, accountability, and explainability) in the development and deployment of the tech – compromising fundamental rights or discriminating against vulnerable persons.

In some countries, the overall utility and efficiency of several of these control measures have also been thrown into doubt as a result of States overpromising the potential of such technologies to eliminate the virus and under-delivering tech potentials. This has had a negative influence on trust and resulting virus containment efforts.

---

[132] 'Over 21,000 Signatures on Petition against Use of S'pore Govt-Issued Wearable Contact Tracing Devices' <https://mothership.sg/2020/06/petition-mandatory-wearable-devices/> accessed 3 September 2020; 'Anti-Maskers Rally as Woolworths and GPs Call for More Mask-Use to Limit Coronavirus' (*SBS Your Language*) <https://www.sbs.com.au/language/english/audio/anti-maskers-rally-as-woolworths-and-gps-call-for-more-mask-use-to-limit-coronavirus> accessed 3 September 2020; Eileen Yu, 'Singapore's Move to Introduce Wearable Devices for Contact Tracing Sparks Public Outcry' (*ZDNet*) <https://www.zdnet.com/article/singapores-move-to-introduce-wearable-devices-for-contact-tracing-sparks-public-outcry/> accessed 11 September 2020.

Ethical pre-requisites for the use of AI-assisted technologies and big data resonate with interests in solidarity, dignity and social responsibility.[133] 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.[134] 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. ***[Covid Regulation paper]***

~

In a recent article entitled 'Can Your Smartphone Crack Covid?'[135] Timandra Harkness, from BBC Radio 4's *Future Proofing and How to Disagree* specifically engages the civil rights issues posed by a variety of Bluetooth tracing and tracking technologies the paper has identified above:

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

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

> The Chinese app, AliPay HealthCode, raises some red flags. It assigns users a unique QR code which displays red, yellow or green, indicating your health status, and which determines how much freedom of movement you're permitted. How that risk category is calculated remains opaque, though it uses proximity to known infected individuals or hotspot locations in that calculation. It sends your identity and location directly to a server accessible by the police, who can use it to enforce the quarantine demanded by your colour status. Use of the app is not compulsory, but even local movement may be impossible without it.

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

---

[133] 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.
[134] Paul Mozur, Raymond Zhong and Aaron Krolik, 'In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags' *The New York Times* (2 March 2020) <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html> accessed 6 April 2020.
[135] Timandra Harkness, 'Can Your Smartphone Crack Covid?' (*UnHerd*, 14 April 2020) <https://unherd.com/2020/04/can-your-smartphone-crack-covid/> accessed 27 April 2020.

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

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

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

In a recent paper published by the Berkman Klein Centre for Internet and Society, and the Health Ethics and Policy Lab[136], the authors identified a typology of digital public health tools devised to tackle the pandemic. [...] the typology spotted proximity tracing, symptom checkers, quarantine compliance tools and flow modelling capacities (the latter which we see instead as analytical enhancements rather than surveillance technology). Particularly helpful is the paper's classification of 'legal and ethical' challenges posed by these innovations and their consequent data usage. Validity, accuracy and necessity, correspond with this papers introductory and prevailing interests in purpose and objective. Privacy, discrimination, public benefit and expiration are common to matters interrogated below. We have treated consent and voluntariness as inextricable from the legal authority for the regulatory impact of these technologies and as such seen then more as concerns when initiating expanded data access. Digital inequality and repurposing are at the heart of fairness considerations and our approach to transparency. The Berkman Klein paper progresses to connect ethical principles (autonomy, beneficence, justice, non-malfeasance, privacy and solidarity)[137] with these identified challenges and from there offers some interesting general recommendations for the ethical use of such public health tools. (...)

The crisis circumstances that the world is facing because of the COVID-19 are being used to justify some of these programmes in the short term. Some of these immediate measures confronting the health crisis have been strongly focused on surveillance, and even though there is a debate whether tracing is surveillance in the narrow sense. At the same time, it is equally

[136] Urs Gasser and others, 'Digital Tools against COVID-19: Framing the Ethical Challenges and How to Address Them' Berkman Klein Centre for Internet & Society, Harvard Law School; Health Ethics and Policy Lab, Department of Health Sciences and Technology, ETH Zürich <https://arxiv.org/ftp/arxiv/papers/2004/2004.10236.pdf>.

[137] In other work soon to be published CAIDG has researched the operational accessibility, relevance and applicability of such high order ethical concepts and concedes that there are significant problems with the translation of this language into practical applications on front-line decision making – see Mark Findlay and Josephine Seah, 'An Ecosystem Approach to Ethical AI and Data Use: Experimental Reflections' (2020) 2020/03 SMU Centre for AI & Data Governance Research Paper <https://papers.ssrn.com/abstract=3597912> accessed 6 January 2021.

important to consider the ethical challenges associated in the medium and long term for data subjects posed by any extension of data storage and use beyond emergency measures. Regardless of the nature of the programmes – whether public, private, permanent or temporal – all tracing initiatives should question the responsible collection and treatment of personal data for the ultimate purpose of the safety of mankind without sacrificing the human dignity of data subjects. ***[Ethics paper]***

~

A pandemic-stricken world has seen state agencies and corporations rushing to collaborate in order to create new forms of digital technologies to curb the spread of the virus, in hopes of curtailing public fears regarding the pandemic's reach. Unsurprisingly, these technologies have also generated some levels of community anxiety and disquiet which is the interest of this paper, not simply as a gauge of community feeling, but as a measurable variable for assessing efficacy and policy relevance. AI-assisted[138] surveillance technology has assumed prominence in the fight against the virus, despite problems associated with its value and impact, compared to more conventional responses like manual tracing, mass testing and social distancing (...)

In the case of inconspicuous surveillance tools undisclosed to the public or data subjects, the regulatory guarantees of transparency, explainability and accountability are even more important if living through the pandemic and post-pandemic control regimes will instil confidence that emergency powers will be just that.[139] Further, the recent global preference for ethics and principled design as sufficient regulatory frames for AI development will come under challenge if their essential elements such as explainability, transparency, accountability and fairness are bypassed in the technological surveillance reliance in COVID-19 control. (...)

Information deficit, lack of transparency and explainability[140]

In situations where data subjects have positively engaged with tracing apps, a lack of transparency and inadequate explanations by the state agencies about how the apps are being used, is common across our research locations. In Singapore, while citizens have expressed a general willingness to participate in having their mobile phones tracked and the corresponding data collected, it remained unclear to respondents in the survey that canvassed consensus *what forms* of data is being collected, and how it is being used. When queried about the control purpose effectiveness of the app's reliance on individual's data, Singapore's Government Technology Agency (GovTech), the developers of TraceTogether, responded to a user: "due to privacy concerns, [they] do not expose stats if there is no real need to do".[141] Confronted with such a reaction from the promoters, the question of what constitutes a "real need" is begged, and what is the threshold of 'real need' that the individual data subject must cross to interrogate their own data, or at the very least scrutinise aggregated information on its use and effectiveness. If the data subject is the enquirer, technological promoters cannot rely on a blanket privacy rebuff and secrecy to detract from explaining data retention and use.

[138] The paper interprets 'AI-assisted' in its broadest understanding so that applications facilitated through smart phone use, we would determine to be within that classification.
[139] For a detailed discussion of these challenges see, Findlay and others, 'Ethics, AI, Mass Data and Pandemic Challenges' (n 95).
[140] Header from original paper.
[141] Reference made to the tables in the Disquiet paper's Appendix.

Similarly, in Australia, there appears to be a correlation between public confidence (reinforced by the government's health authorities via daily updates and information on transmission and fatalities),[142] and the uptake of the COVIDSafe app. However, confidence in COVIDSafe itself appears to be lacking, as the Australian government has not published information and studies evaluating whether the COVIDSafe system is achieving its objectives, or whether it is even credible and necessary.[143]

In Southeast Asia, Indonesia's PeduliLindungi[144] surveillance app also raised questions over the safety of the storage of personal data on smart phones. An open letter collated by 13 human rights organisations was transmitted to the Indonesian Minister of Communication and Information Technology requesting strong user privacy protections.[145] In this letter, guarantees were sought for greater transparency, such as the release of the white paper and source code of PeduliLindungi under an open source license to enable independent experts to examine potential vulnerabilities. In this case, the issue of transparency was particularly problematic as there is no privacy policy available for the app on either Apple's App Store or Google's Play store. Recognising privacy as a fundamental right, the open letter called on relevant regulation, as well as for the specifications of the technology to be spelled out confirming the measures taken to protect individuals' data from cyberattacks and security breaches.[146] Similarly, 18 organisations wrote an open letter to the Philippines' government, making analogous requests for strong user protections over its StaySafe.ph's app.[147]

Derivative frustration felt by users at the lack of transparency and accountability by government bodies may also exacerbate the distrust towards the state in the wider exercise of its control functions.[148] While indicative of prevailing sentiment, we nonetheless note that selected comments comprising public reviews of certain apps do not necessarily represent aggregate opinions of individual users of the app. Those with a deeper appreciation for app's utility may have a different reaction to and evaluation of the use of the tracking app. (...)

Accountability of authorities[149]

Governmental miscommunication surrounding the introduction of control technology in other jurisdictions has further fuelled public confusion. For instance, in the UK, while the NHSX's test and trace app was initially set to launch in May across the country, this never eventuated

[142] Australian Government Department Health, 'Coronavirus (COVID-19) Health Alert' (*Australian Government Department of Health*, 6 February 2020) <https://www.health.gov.au/news/health-alerts/novel-coronavirus-2019-ncov-health-alert> accessed 6 August 2020.
[143] Greenleaf and Kemp (n 109).
[144] The Kominfo had launched the PeduliLindungi tracing app on 14 April 2020. Mahinda Arkyasa, 'Kominfo Launches COVID-19 Tracking App' (*Tempo*, 14 April 2020) <https://en.tempo.co/read/1331513/kominfo-launches-covid-19-tracking-app> accessed 1 September 2020.
[145] 'Indonesia: Open Letter to KOMINFO Requesting Strong User Privacy Protections for Contact Tracing App' (*ARTICLE 19*) <https://www.article19.org/resources/indonesia-open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/> accessed 5 August 2020; 'Open-Letter-PeduliLindungi-ENG.Pdf' <https://www.article19.org/wp-content/uploads/2020/06/Open-Letter-PeduliLindungi-ENG.pdf> accessed 5 August 2020.
[146] 'Indonesia: Open Letter to KOMINFO Requesting Strong User Privacy Protections for Contact Tracing App' (n 145).
[147] 'Open Letter to Request for Strong User Privacy Protections in the Philippines' COVID-19 Contact Tracing Efforts' (*DigitalReach*, 9 July 2020) <https://digitalreach.asia/open-letter-to-request-for-strong-user-privacy-protections-in-the-philippines-covid-19-contact-tracing-efforts/> accessed 5 August 2020.
[148] Findlay, Milne and Palma (n 93).
[149] Header from original paper.

as developers encountered Bluetooth performance obstacles.[150] Part of the launch's fiasco was attributed to Apple's unwillingness to make an exception for the United Kingdom's government to allow the app to use Bluetooth in the phone's background. The government then switched efforts to manual contact tracing practices, but promised a "world beating" tracing system to be released in early June.[151] When queried again on 5 June 2020, Minister Nadhim Zahawi admitted that he could not give an exact release date for the app.[152] Subsequently, Lord Bethell, Minister for Innovation at the Department of Health and Social Care, predicted that the app would be launched in winter of 2020 as it was "not a priority for the government" and that they were not fazed by the time pressure.[153] Finally on 18 June 2020, it was revealed that the government had abandoned the centralised app and substituted it with the decentralised Apple-Google model.[154] The chaotic mismanagement of the contact tracing app has been labelled as a debacle,[155] with many demanding an explanation as to why publicly aired enquiries remain unaddressed and dismissed.[156] (...)

Overselling and overpromising the privacy-protection capacities of technologies[157]

Technology sponsors have repeatedly made unsubstantiated or unreasonable guarantees regarding the privacy protections inherent in their applications, particularly those operating via Bluetooth connectivity.[158] Overselling the capacities of such technologies in these instances, paired with a wider public misunderstanding of the capabilities and limits of current technologies, will only breed distrust – both in the device and in the authority on which it rests.

Doubts, founded in an absence of knowledge and fear (aggravated by the lack of clear communication), are also exacerbated by untrustworthy practices. For example, surveillance companies have allegedly faked their software demonstrations,[159] and contact tracing apps like Norway's Smittestopp[160] carried out live or near-live tracking of users' locations and uploaded GPS coordinates to a central server. Such conduct was initially unknown to the Norwegian

[150] Leo Kelion, 'Ministers Consider Coronavirus-Tracing App Rethink' *BBC News* (11 June 2020) <https://www.bbc.com/news/technology-52995881> accessed 3 August 2020.
[151] Rory Cellan-Jones, 'What Went Wrong with the Coronavirus App?' *BBC News* (20 June 2020) <https://www.bbc.com/news/technology-53114251> accessed 3 August 2020.
[152] 'NHS Virus Tracing App "in Place by End of Month"' *BBC News* (5 June 2020) <https://www.bbc.com/news/uk-52931232> accessed 3 August 2020.
[153] Sarah Boseley, 'NHS Covid-19 Contact-Tracing App for UK Will Not Be Ready before Winter' *The Guardian* (17 June 2020) <https://www.theguardian.com/society/2020/jun/17/nhs-covid-19-contact-tracing-app-no-longer-a-priority-says-minister> accessed 3 August 2020.
[154] Leo Kelion, 'UK Virus-Tracing App Switches to Apple-Google Model' *BBC News* (18 June 2020) <https://www.bbc.com/news/technology-53095336> accessed 3 August 2020.
[155] 'The UK's Contact Tracing App Fiasco Is a Master Class in Mismanagement' (*MIT Technology Review*) <https://www.technologyreview.com/2020/06/19/1004190/uk-covid-contact-tracing-app-fiasco/> accessed 3 August 2020.
[156] James Vincent, 'Without Apple and Google, the UK's Contact-Tracing App Is in Trouble' (*The Verge*, 5 May 2020) <https://www.theverge.com/2020/5/5/21248288/uk-covid-19-contact-tracing-app-bluetooth-restrictions-apple-google> accessed 3 August 2020.
[157] Header from original paper.
[158] Stephen White, '#privacy: Bluetooth Offers a Cyber-Security Window for the Hackers' (*PrivSec Report*, 22 August 2019) <https://gdpr.report/news/2019/08/22/bluetooth-offers-a-cyber-security-window-for-the-hackers/> accessed 6 August 2020.
[159] 'Artificial Intelligence Won't Save Us From Coronavirus' *Wired* <https://www.wired.com/story/artificial-intelligence-wont-save-us-from-coronavirus/> accessed 22 July 2020.
[160] The Smittestopp app was launched on 16 April 2020. 'Norway Launches "smittestopp" App to Track Coronavirus Cases' (16 April 2020) <https://www.thelocal.no/20200416/norway-launches-smittestop-app-to-track-coronavirus-cases> accessed 1 September 2020.

public who then later criticised this practice as being too invasive of privacy, upon discovery.[161] Aligned with the resistance of this sort in Norway is fear that private and public data harvesters are partnering and using data for purposes not originally consented to by data subjects (particularly when drawn from social media platforms that possess privacy protection policies). With contact tracing apps emerging worldwide, critics consider whether trust-by-design or privacy-by-design models on which many of the apps are purportedly built can fulfil their purpose in mitigating public suspicions and distrust by requiring the ethical compliance of promoters.[162]

Distrust in the technology and its promoters and their motives may remain below the surface of public dissent long after the voices of disquiet die out. Against suppressed concerns about the perpetuation of surveillance states, particularising the immediate and ongoing efficacy of pandemic control policies reliant on mass surveillance, and their capacity to effectively pre-empt new waves or future pandemics, while at the same time vigilantly guarding against 'surveillance creep', may be preferable to social distancing ongoing.

Especially in situations of digital contact tracing, privacy breaches, particularly with non-aggregated personal data, are inevitable if there are insufficient safeguards put in place.[163] As a response to privacy concerns, Apple and Google's partnership in the creation of the Exposure Notification System[164] utilises a "decentralised" approach which is commended for data collection without a centralised database,[165] thereby effectively limiting the consequences that arise from data breaches in a single large repository.

Effectiveness and functionality of technologies[166]

In countries with tracing and tracking policies, despite wide-scale state promotion and some attempts at public education regarding the operation of contact tracing technology, multiple reports have revealed citizens' reluctance to download the apps, with many expressing apprehensions towards the technology inherent to the devices.

For instance, these worries are evident in the complaints that surface on Chinese social media over inaccuracy of the apps operations.[167] The Health Code (which users can sign up for via AliPay and WeChat) functions on a green-yellow-red scheme, which operates on a scale indicating to users that they are free to travel; should be in home isolation; or are confirmed to be COVID-19 patients, respectively. Several users have reported that they were unable to rectify erroneous "red" designations which were left uncorrected even after officials were

[161] 'Should I Worry about Mass Surveillance Due to COVID-19?' <https://newseu.cgtn.com/news/2020-07-03/Should-I-worry-about-mass-surveillance-due-to-COVID-19--RNQLZgoHWE/index.html> accessed 20 July 2020.
[162] Gerard Goggin, 'COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology' (2020) 177 Media International Australia 61.
[163] Sharon (n 61).
[164] 'Privacy-Preserving Contact Tracing - Apple and Google' (*Apple*) <https://www.apple.com/covid19/contacttracing> accessed 30 July 2020.
[165] Sam Schechner and Jenny Strasburg, 'Apple, Google Start to Win Over Europe to Their Virus-Tracking Technology' *Wall Street Journal* (20 May 2020) <https://www.wsj.com/articles/apple-google-start-to-win-over-europe-to-their-virus-tracking-technology-11589716800> accessed 1 October 2020.
[166] Header from original paper.
[167] It is useful to remember that there exist two realms of social disquiet in authoritarian states – limited public expression of dissent is tolerated but vigorous social media commentary is impossible to repress.

alerted to such a problem,[168] leaving many to question the accuracy of such surveillance and the genuine utility of their related apps.[169]

As discussed earlier, the utility of contact tracing apps also came under heavy scrutiny in the United Kingdom as the government failed to successfully deploy its proclaimed centralised model NHS-developed app.[170] From the beginning, the centralised approach, favoured for its potential to help identify patterns and detecting clusters, faced criticism from privacy and security experts as the breach of data in a centralised system would result in wide-ranging harms. Technical difficulties also plagued the app during the trial, with reports of data-input problems; the app's inability to identify nearby users as a single person; and instances of several patients in England being sent to testing sites located in Northern Ireland.[171] Despite the appeal of such apps, initial research has suggested that these technologies (centralised or decentralised) have not significantly aided the contact tracing process.[172]

Singapore's new self-check system[173] will potentially see a growth of false positive numbers as is already evident in exposure notification apps,[174] involving circumstances of highly improbable situations for users to be exposed. As users are wrongly notified about a genuine risk of infection the heightened anxiety generated from these false positives weakens the trust of data subjects in both the technology and its state promoters.[175]

More surprising is the fact that apart from data subjects and experts, the efficacy of contact tracing apps is also called into question by state officials themselves. In Australia, Victorian agencies confirmed that they had stopped using COVIDSafe (which they attributed to community pressure)[176] while the country's second wave grew. Grim pronouncements by experts recognised such a move as being a significant factor in the rise of community spread.[177] The authorities evidently struggled to reconcile the digital app with manual contact tracing efforts, choosing instead to cease its operations, thereby rendering the app's tracing algorithm inoperable. This capitulation by Victoria rejecting technology in the face of often-misguided citizen resistance and thereby reducing control capacity demonstrates that without concerted efforts to enhance explainability, the opacity of the technology and the absence of positive

---

[168] 'China's Coronavirus Health Code Apps Raise Concerns over Privacy' (*the Guardian*, 1 April 2020) <http://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy> accessed 22 July 2020.
[169] 'China's Coronavirus Health Code Apps Raise Concerns over Privacy' (n 168).
[170] Cellan-Jones (n 151).
[171] 'The UK Is Abandoning Its Current Contact Tracing App for Google and Apple's System' (*MIT Technology Review*) <https://www.technologyreview.com/2020/06/18/1004097/the-uk-is-abandoning-its-current-contact-tracing-app-for-google-and-apples-system/> accessed 3 August 2020.
[172] Isobel Braithwaite and others, 'Automated and Partly Automated Contact Tracing: A Systematic Review to Inform the Control of COVID-19' (2020) 0 The Lancet Digital Health <https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30184-9/abstract> accessed 22 August 2020.
[173] 'Strengthening Measures for Safe Reopening of Activities' <http://www.gov.sg/article/strengthening-measures-for-safe-reopening-of-activities> accessed 10 September 2020.
[174] 'The Importance of Equity in Contact Tracing' (*Lawfare*, 1 May 2020) <https://www.lawfareblog.com/importance-equity-contact-tracing> accessed 24 September 2020.
[175] Mark Findlay and others, 'Strengthening Measures for Safe Reopening of Activities: Ethical Ramifications and Governance Challenges'.
[176] Chris Duckett, 'Victoria Ditched COVIDSafe App but Is Using It Again' (*ZDNet*) <https://www.zdnet.com/article/victoria-ditched-covidsafe-app-but-is-using-it-again/> accessed 6 August 2020.
[177] David Crowe, 'Victorian Officials Stopped Using COVIDSafe App as Second Wave Grew' (*The Sydney Morning Herald*, 4 August 2020) <https://www.smh.com.au/politics/federal/victorian-officials-stopped-using-covidsafe-app-as-second-wave-grew-20200804-p55ihd.html> accessed 4 August 2020.

counter-messages affects both trust and safety. Compromised public trust resulting in community resistance against tracking/tracing technologies and forcing the large-scale abandonment of assistive technology has negative control ramifications, particularly when technology assists manual control practices. While Victoria has since resumed its use of COVIDSafe, it is probable that the delay before the re-implementation of the app and associated negative impacts on community confidence have unfortunately contributed to the soaring second wave of infections and the necessary imposition of much more intrusive control responses like the imposition of a state-wide militarised curfew.[178] (...)

There is a practical and pressing need for an increase in transparency around how the surveillance technologies are deployed, as well as clarity about how data is collected and used. Only by informing the public when and how technical flaws are being addressed and explaining the facts behind the workings and status of the technology will the public be comforted by the sincere efforts of the agencies' data management. Where the citizen/data subject is integrated in control policy, an environment of compliance and trust will be fostered among and between the community and the state, which would reduce the need for the state to then resort to coercive methods demanding citizen compliance.[179] (...) ***[Disquiet paper]***

3.6 The dangerous merger of the public and private

To maximize all available resources and personnel in this health crisis, governments around the world have resorted to forming various public-private partnerships. Yet, these partnerships are not without their own complications. Across the papers below, authors identify some dangers that have or will arise out of the merger between big and private tech companies and public agencies. Issues such as informed consent, the repurposing and monetization of citizens' personal data, and concentration of power in the hands of technological giants are recurrent themes for further scrutiny.

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. [***Covid Regulation Paper***]

~

Apart from personal disquiet expressed by data subjects who have directly interacted with the surveillance technologies, experts have expressed apprehensions surrounding the concentrated control of computing infrastructure and its implications on the existing power asymmetries between private tech companies and public agencies. This reservation reflects the reality of big

[178] 'Australia's Victoria State to Deploy Military, Impose A$5,000 Fines to Enforce Coronavirus Isolation' (n 113).
[179] 'Australia's Victoria State to Deploy Military, Impose A$5,000 Fines to Enforce Coronavirus Isolation' (n 113).

technological companies encroaching into territories of political and medical policy. In Dr Tamar Sharon's view: [180]

> In the context of a pandemic, where human proximity is the primary threat, the dependency on infrastructures for mediated and remote human contact—telehealth, communications services, cloud storage—is amplified (Klein 2020). This can lead to a reshaping of these sectors to align with the values and interests of non-specialist private actors, which may or may not be the interests and values of those groups and individuals who should immediately benefit from the distribution of goods in those spheres, be they patients, students, residents of a city, or more generally speaking, citizens.

This is illustrated in France, where French officials reported that when they had tried to approach Apple and Google with their centralised protocol for contact tracing to see if an accommodation could be reached, they were met with "staunch reaffirmations that the companies would only work with decentralised technologies".[181] The ability of tech giants like Apple and Google to dictate the kinds of apps they would upload, regardless of the state's authority, exemplifies the power unevenness between tech companies and public agencies even in crisis contexts. Instead of working together, the states appear to need to work around the decentralised framework that the Apple-Google protocol provides, rather than having these private companies recognising the authority of the states and accommodating their protocol. This exercise of private commercial power demonstrates via technological advantage private companies leverage their ability to negotiate into the realm of political responsibility on an international scale.[182] Dr Sharon states,

> In this case, a legitimate advantage acquired in the sphere of digital goods— digital expertise—has been converted into advantages in the sphere of health and medicine (where epidemiological expertise should be the main source of legitimacy), and in the sphere of politics (where democratic accountability should be the source of legitimacy). Each of these transgressions presents its own risks. Namely, a crowding out of essential spherical expertise, new dependencies on corporate actors for the delivery of essential, public goods, the shaping of (global) public policy by non-representative, private actors and ultimately, the accumulation of decision-making power across multiple spheres. [183]

Moreover, private tech giants are not held to high standards of open scrutiny despite their extensive collection and use of data while governments bear the brunt of public distrust and suspicion, and are called to account through democratic processes not required of the private sector. Given that states must rely on data provided by private corporations (e.g. utilising contact data provided by telecommunications operators (telcos) to send texts to inform those who have been exposed to the virus), these companies should likewise be held to comparable levels of accountability when operating in tandem with state agencies.[184] This responsibility is mutualised because of the data shared in the public and private agencies. That said, much background data came into the private sphere for purposes and under consent regimes that had

[180] Tamar Sharon, 'Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers' [2020] Ethics and Information Technology 1.
[181] Sharon (n 180).
[182] Sharon (n 180).
[183] Sharon (n 180).
[184] Morgan Meaker, 'The Original Big Tech Is Working Closer than Ever with Governments to Combat Coronavirus – with No Scrutiny' (*The Correspondent*, 5 August 2020) <https://thecorrespondent.com/621/the-original-big-tech-is-working-closer-than-ever-with-governments-to-combat-coronavirus-with-no-scrutiny/81373317498-76dea099> accessed 17 August 2020.

nothing to do with pandemic control. For this reason the private actors have obligations to data subjects that are outside the exigencies of the pandemic.

The power of representative state agencies can also attempt to capture private sector capacity, evidenced where local private sector operators have resisted government directives to divulge personal data. During the March 2020 elections, GUILAB SA, Guinea's telco, was ordered to carry out network repairs during that particular weekend. GUILAB's management refused, assuring the public that maintenance works would only be postponed till after the elections, which served to assuage fears of election interference.[185]

The growing encroachment by technological conglomerates into political and medical spheres is a phenomenon that requires greater attention, especially since the tech giants' commercial interests may not necessarily overlap with the policy imperatives of political and medical experts. It becomes important for stakeholders to be aware of, and take concerted steps to limit the extent of commercial influence over arenas of public decision-making.[186] [***Disquiet Paper***]

3.7 Sectorial-specific challenges

3.7.1 Disconnect between financial markets and the economy

In the pandemic, investors, like all responsible citizens, share an obligation to keep the community safe. This obligation extends to informed market decision-making that goes beyond one's own self-interest. However, as Findlay demonstrates in his *Polanyi paper*, this has unfortunately and regrettably been ignored. The excerpts below will expand on the current disconnect between financial markets and the economy and suggest that the disconnect cannot just be explained by the different purposes of economic and financial market analysis but rather by the informational indicators they rely on.

Introduction - the Paradox:

> Is anything strange about the stock market behaviour in the time of COVID-19? As the world suffered from the worst economic crisis since the Great Depression (Baldwin and Weder di Mauro 2020a, 2020b, Bénassy-Quéré and Weder di Mauro 2020, Coibon et al. 2020)[187], the reaction of stock markets raises serious concerns. Since the beginning of the crisis, stock prices seem to be running wild. They first ignored the pandemic, then panicked when Europe became its epicentre. Now, they are behaving as if the millions of people infected, the 400,000 deaths (as in June 2020), and the containment of half the world's population will have no economic impact after all.[188]

[185] 'Internet Cut across Guinea Ahead of Elections' (*NetBlocks*, 20 March 2020) <https://netblocks.org/reports/internet-cut-across-guinea-ahead-of-elections-xAGoQxAz> accessed 17 August 2020.
[186] Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (Columbia Global Reports 2018).
[187] Richard E Baldwin and Beatrice Weder di Mauro, *Economics in the Time of COVID-19* (CEPR Press 2020) <https://voxeu.org/system/files/epublication/COVID-19.pdf> accessed 8 January 2021.
[188] Gunther Capelle-Blancard and Adrien Desroziers, 'The Stock Market and the Economy: Insights from the COVID-19 Crisis' (*VoxEU CEPR*, 19 June 2020) <https://voxeu.org/article/stock-market-and-economy-insights-covid-19-crisis> accessed 8 January 2021.

In Paul Krugman's view;

> Whenever you consider the economic implications of stock prices, you want to remember three rules. First, the stock market is not the economy. Second, the stock market is not the economy. Third, the stock market is not the economy (…). The relationship between stock performance – largely driven by the oscillation between greed and fear – and real economic growth has always been somewhere between loose and non-existent.[189]

Whether an explanation lies in that during the economic strains of the pandemic there are limited investment options, and as such stock trading is resorted to,[190] or that stock trading is more tied to stakeholder 'confidence' than to genuine facts, shareholders seem less troubled by the cataclysmic infection and death figures than they are impressed with the stimulus intervention of central banks.[191] It seems clear that many investors have not been seriously factoring into their trading decisions either the economic fragility of the jurisdictions in which they operate, or particular disease transmission vectors and measures of strategic social vulnerability. [192] On the other hand, government financial guarantees, social distancing lockdowns, lower policy interest rates and employment protection are approached as mitigating declines in stock prices, rather than essential health concerns.

Any fall in the financial market presently is not said to be a consequence of an asset bubble but rather of an interruption in economic activity to fight the disease. Factor in a reflection on profit returns as 'from now to infinity' rather than now till economic recovery out of the virus (if it comes) and financial markets adopt a more optimistic predictive tone than economic and social facts would justify. In addition, any suggested collapse in the financial sector is not now, like there was in 2008-9, the evil consequences of risky bank speculation, and as such governments are more willing to assist the financial industry with credit support and relief, and the voting public is more prepared to accept this approach. And on firm valuation, earlier company buy-back schemes have comforted the market that valuations during the crisis and beyond are realistic. Ultimately there may be a sense that panic and the fire-sale buying which attends it is not the best approach for medium term financial gains.[193]

However one reads the tea leaves, if the wild fluctuations in the stock markets worldwide during the progress of the pandemic are any indication, and stock markets can be said to represent financial markets in all there forms which is contestable, there is no doubt a huge disconnect between financial market progressions and radical declines in all major economic pointers. In his article 'The US is in a recession, but the stock market marches higher: Here's

---

[189] Paul Krugman, 'Crashing Economy, Rising Stocks: What's Going On?' *The New York Times* (30 April 2020) <https://www.nytimes.com/2020/04/30/opinion/economy-stock-market-coronavirus.html> accessed 8 January 2021.

[190] Robert Shiller and Burton Malkiel, 'Does Covid-19 Prove the Stock Market Is Inefficient?' (*Pairagraph*, 2 May 2020) <https://www.pairagraph.com/dialogue/c93c449006c344ce94e6e2e8fbe7aba3> accessed 8 January 2021.

[191] Capelle-Blancard and Desroziers (n 188).

[192] Capelle-Blancard and Desroziers (n 188).

[193] Theo Vermaelen, 'COVID-19: Four Reasons for Optimism About the Stock Market' (*INSEAD Knowledge*, 23 April 2020) <https://knowledge.insead.edu/blog/insead-blog/covid-19-four-reasons-for-optimism-about-the-stock-market-13896> accessed 8 January 2021.

why there is a disconnect', Greg Iacurci, while reiterating that the stock market is not the economy, explains it as a mix of internalised market confidence and hopeful prediction:[194]

> The Covid-19 public health crisis pushed states to shutter broad swaths of their economies…
>
> Nearly 43 million Americans have since filed for unemployment benefits, shattering prior records.
>
> The country's 14.7% official unemployment rate in April was its highest level since the Great Depression, when it peaked above 25%. The rate rebounded to 13.3% in May after the economy added 2.5 million jobs during the month, but some economists are sceptical that trend will continue.
>
> Stock investors are looking beyond present conditions toward what they believe will happen in the future — which they're currently viewing with optimism, experts said… A 34% decline in the S&P 500 wasn't reflective of the pandemic's likely effect on the long-term U.S. economy, said Preston Caldwell, senior equity analyst at Morningstar. (Caldwell observed)
>
> "I would say the economic data is old news for the market's purposes," Caldwell said.
>
> "Right now, most market participants are looking beyond the [second quarter] to try to understand the second half of 2020 and beyond."

Absent the recognition of a rich mine of contrary data on which financial advisers can qualify their rosy predictions this is a story of two different realities – or perhaps one harsh reality and one expectant gamble. The resultant disconnect cannot just be explained by the different purposes of economic and financial market analysis *but rather by the information indicators on which these rely*. Financial markets manipulate internally generated information (about things like financial product) to calibrate and monetise risk. Economic forecasting is more likely to rely on external variables that reveal the state of essential economic relationships (such as employment figures and job vacancies). (...)

As a point of explanation, some might argue that speculation itself is not a problem, provided it does not degenerate into market manipulation. Therefore, short-selling could represent nothing more than a valid market strategy within the permits of legitimate trading. Here I do not advance a critique of speculation in general. However, attitudes to the information on which speculation is based have shifted radically in times of crisis. For instance, as a consequence of financial turmoil in the 1980's most jurisdictions moved to criminalise insider trading. In the spirit of regulating out of crisis to ensure market sustainability, the argument here is that regulators are well advised to focus on the nature and impact of information stimulating speculation and determine if and how such information needs to be viewed as a risk factor working against sustainability and resilience. (...)

[194] Greg Iacurci, 'The U.S. Is in a Recession but the Stock Market Marches Higher. Here's Why There's a Disconnect' *CNBC* (3 June 2020) <https://www.cnbc.com/2020/06/03/understanding-the-huge-disconnect-between-the-stock-market-and-economy.html> accessed 8 January 2021.

[...] the explanation for this dangerous disconnect can be found in Karl Polanyi's understanding of fictitious commodities in self-regulating markets, dis-embedding from the social and his propositions for market correction through the double movement.

Polanyi's theoretical frame offers a clearer understanding of how, when markets move further away from genuine social utility, they represent threats to social stability which short-term wealth generation does not counterbalance. (...)

Karl Polanyi published, 'The Great Transformation: the political and economic origins of our time'[195] in the final year of World War II, about the same time as Hayek's 'The Road to Serfdom' appeared, which was the driving force behind the free-market revolution in the final quarter of the 20th century. Polanyi, on the other hand, using the transformation from the industrial revolution as his backdrop, explained the deficiencies of the self-regulating market[196] (writ so large in the 2008-9 global financial crisis), and the potentially dire social consequences of un-tempered market capitalism. The importance of his thinking in an era of globalisation under challenge, free trade in retreat and the dislocation of financial markets from the economy, cannot be underestimated.[197]

Instead of positioning the social and the economic as two polar opposites, compelling a choice of one over the other, Polanyi's theory focuses on the interconnectedness between the two and the manner in which this has been strained. For Polanyi, the economic system was never entirely separated from the social.[198] Polanyi recognized the importance of both the social and economic spheres and their duality manifested in various stages of embeddedness, a concept we recognize is not free of criticism to which we will return subsequently.

When addressing the failings of neo-liberal market economies, and the disconnect between financial markets and the economy at large, Polanyi's interest in economic anthropology is useful on at least two levels.[199] The first is to explain the dis-embedding of property and its markets in which fictitious commodities such as land, labour and money are cultivated. The second is to determine whether a modern critique of property and its markets can be removed from a capitalist market environment. At the centre of such an exploration is his concern about how property, as the product of labour becomes disconnected from society. The relevance of Polanyi's theory lies in how it maps out the shift from a state of embeddedness to one of dis-embeddedness (as characterized by financial markets and the more general the market economy), prompting resistance by society as it seeks to re-embed the market back into the social. (...)

Adopting Polanyi's explanation that the movement in market economies away from the social requires and results in fictitious commodification, then the binary fictitious/real (actual) will

---

[195] Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time* (Beacon Press 2001).

[196] Explaining self-regulating markets, when some might respond that financial markets are already significantly regulated, much of the regulatory 'back-bone' in financial markets as I see it still reverts back to the exercise of investor discretion even where that discretion may be confined. It is what Julia Black refers to as constitutionalising self-regulation. Julia Black, 'Constitutionalising Self-Regulation' (1996) 59 The Modern Law Review 24.

[197] Discussed at length in Mark Findlay, *Law's Regulatory Relevance?: Property, Power and Market Economies.* (Edward Elgar Publishing 2017).

[198] Polanyi (n 195) 70.

[199] Polanyi (n 195); Duran Bell, 'Polanyi and the Definition of Capitalism' in Jean Ensminger, *Theory in Economic Anthropology* (AltaMira Press 2002).

necessitate the real as the social and the fictitious as self-regulating markets cut free from fundamental social bonding.

What is meant by fictitious can be seen in Jessop's interpretation of Polanyi:

> …a fictitious commodity has the form of a commodity (can be bought and sold) but is not actually produced to be sold. It exists already before it acquires the form of an exchange value (eg. raw nature) or it is produced as a use value before being appropriated and offered for sale…a fictitious commodity is not created in a profit-oriented labour process subject to competitive pressures of market forces to rationalise its production and reduce the turnover time of invested capital…[200]

Therefore, fictitious commodities and their markets do not obey rules such as that of pure competition, normatively declared by capitalism. In terms of, for instance the information economy, we can see the influence of social scarcity in an artificial rather than a real vein. Law at present is actively involved in the enclosure of collectively produced knowledge (and does so in exchange market regulation through limiting some forms of privileged information from trading decisions). As a result, knowledge is:

> …codified, detached from manual labour and disentangled from material products to acquire independent form in expert systems, intelligent machines, or immaterial products and services.

From this characterization, Jessop returns to the dis-embedding of commodities if knowledge in certain market contexts can be seen as fictitious:

> …knowledge is dis-embedded from its social roots and integrated into extra-economic institutional orders, functional systems, and the lifeworld and made subject to creeping commodification so that the primary code governing its use is profitable/unprofitable rather than true/false, sacred/profane, health/disease et cetera.[201]

Along with law's responsibility in this age of change there will be an adjunct necessity for an extension of market organization to work in favour of what Jessop refers to as genuine rather than fictitious commodities. Discussions for achieving this in terms of requiring risky financial product to be explained to potential investment intensified after the 2009-9 financial collapse. This process, therefore, is more than an ideological intent.

> This self-regulating market of economic liberalism is opposed by social protection intended to preserve man and nature. This is Polanyi's famous double movement.[202]

Polanyi singled out the essential elements of the market, namely, labour, land and money as fictitious commodities,[203] elements that are not produced for sale yet playing a pivotal role in

---

[200] Bob Jessop, 'Knowledge as a Fictitious Commodity: Insights and Limits of a Polanyian Perspective' in Ayşe Buğra and Kaan Ağartan (eds), *Reading Karl Polanyi for the Twenty-First Century: Market Economy as a Political Project* (Palgrave Macmillan US 2007) <https://doi.org/10.1057/9780230607187_7> accessed 1 July 2021.
[201] Jessop (n 200) 120.
[202] Jessop (n 200) 117.
[203] Polanyi (n 195) 75.

the market. *Money*, for instance, is merely a token of purchasing power which, as a rule, is not produced at all, but comes into being through the mechanism of banking or state finance".[204]

Polanyi analysts such as Jessop have recently proposed a reconsideration of commodities which might be deemed fictitious, as well as for a more nuanced reflection on the processes of market dis-embedding through fictitious commodification.[205] In relation to the latter, Jessop advances, on the way to evaluating whether *knowledge* might now be seen as a fictitious commodity, a five-stage commodification format: pre-commodification, fictitious commodification, quasi-commodification, real commodification and fictive capital. These different commodification forms are said to better cover fictitious market transformation in a globalised economy.

Bringing Polanyi back to considering the disconnect between the financial markets and the economy in this time of pandemic the following observations follow:

- The economy has dis-embedded from the social so that disease mass infection translates into economic collapse, due in part to the impact of revaluing fictitious commodities in exchange markets;
- The financial markets have dis-embedded from the economy because financial markets transact quasi commodities which are income generating instruments and relationships not requiring any connection to social reality;
- The financial market generates wealth through trading fictive capital which is an imaginary creation of the market. As such there is less need for the financial market to reflect the trends in an economy which ultimately returns to the means of production;
- If knowledge/information can be viewed as a fictitious commodity then it can service any market if the primary code governing its use is profitable/unprofitable rather than true/false (sacred/profane, health/disease);
- Knowledge/information can dis-embed further from the social and service fictitious commodities more detached from the social, when markets are more self-regulated.

As such the disconnect between the financial market and the economy in times of pandemic is not so much a paradox but a product of different degrees of dis-embedding and fictitious commodification. However, as the double movement asserts, no exchange market will ever absolutely dis-embed from the social and therefore counter-movements such as a pandemic disease can reign in even the most self-regulated markets if those social essentials for the market re-assert themselves (such as a sustainable human/natural environment within which market trading can occur). ***[Polanyi paper]***

3.7.2 The evolution of data-driven finance: Implications for the banking sector

Although the COVID-19 pandemic has halted the operation of many industries, it did not have the same hard-hitting impact on the data-driven finance world. In the excerpts below, Remolina expands on the acceleration of the data-driven transformation in the financial services industry, demonstrating how traditional financial institutions and Fintechs leveraged on data-driven solutions to respond to pandemic-related challenges. Although such solutions can contribute to the recovery of the economy, Remolina also

[204] Polanyi (n 195).
[205] Jessop (n 200).

cautioned that it is necessary to acknowledge the potential risks and challenges posed to consumer protection and financial stability.

Data has taken immense importance in the last few years. Considering the amount of data that is being collected worldwide every day[206], industries are reshaping their activities to become data driven businesses. The *datafication* of almost any aspect of human social, political and economic activity is a result of the information generated by the numerous daily routines of digitally connected individuals and technology. The financial services industry is not isolated from this trend. This vast sea of data, that can now be stored, organised and made sense of for the industry, and a set of emerging tools and approaches, could broadly be called as data-driven finance and is already driving the next wave of innovation and optimisation in the financial sector.[207] (...)

This intersection of finance and data generates benefits for the financial sector. It brings more competition that will ultimately benefit consumers, makes the system more efficient in terms of operation costs, might help financial services providers to meet their customers' needs better and enhance their risk management.[208] (...)

Even though COVID-19 may have slowed our daily lives and stopped the operation of many industries, it did not have the same effect in the data-driven finance world. Not only did health authorities in many jurisdictions leverage the control of the pandemic with data-driven initiatives,[209] but the financial sector and fintech companies are also finding ways to use data to respond to the challenges posed by the pandemic, especially the demands of the economy in these uncertain times. This section shows how some use cases of data-driven fintech accelerated because of the pandemic: (...)

Data-driven lending to help Small and Medium Enterprises (SMEs)[210]

(...) the pandemic has severely impacted small businesses around the world. Businesses are facing unprecedented economic disruption, losses, and are compelled to adapt to new ways of working.[211] With these unforeseen challenges, governments are offering financial assistance in the form of relief loan packages, designed to help small businesses navigate the crisis.[212] Most

---

[206] By 2020, about 1.7 megabytes a second of new information will be created for every human being on the planet. Thus, Data is set to rise steeply to 44 zettabytes by 2020. To put that in perspective, if each Gigabyte in a Zettabyte were a brick, 258 Great Walls of China (made of 3,873,000,000 bricks) could be built. There are 931322574615.48 gigabytes in a zettabyte. See Amit Garg and others, 'Analytics in Banking: Time to Realize the Value' (*McKinsey & Company Financial Services*, 11 April 2017) <https://www.mckinsey.com/industries/financial-services/our-insights/analytics-in-banking-time-to-realize-the-value> accessed 7 January 2021; Thomas Barnett Jr., 'The Zettabyte Era Officially Begins (How Much Is That?)' (*Cisco Blogs*, 9 September 2016) <https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that> accessed 8 January 2021.

[207] See Garg and others (n 206).

[208] Dirk A Zetzsche and others, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) 14 New York University Journal of Law and Business 393.

[209] Findlay and Remolina (n 57).

[210] Header from original paper.

[211] 'Coronavirus (COVID-19): SME Policy Responses' (*OECD*, 15 July 2020) <http://www.oecd.org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/> accessed 20 July 2020.

[212] 'Coronavirus (COVID-19): SME Policy Responses' (n 211).

of these packages are allocated through banks around the world. Regulators have also decided to allow banks to use their capital buffers to provide more liquidity to the economy in forms of loans. [213]

Consequently, banks are getting inundated with a massive volume of loan application requests from small businesses, all of which must be reviewed and approved in a short time. Processing of loan application requests involves multiple steps, from loan underwriting to verification checks and approvals. [214] There also needs to be a mechanism to authenticate the small business enterprises applying for the loan, by extracting critical data needed for approving the loan application. The failure to process loan application requests on time leads to a huge backlog, customer dissatisfaction and a negative impact in the recovery of economies. In some countries, traditional banks have been criticized because of their slow response to COVID-19, particularly in relation to lending issues.[215] (...)

To address this issue, some jurisdictions[216] allowed non-bank online lenders that use Artificial Intelligence and Machine Learning models for lending and credit scoring – to participate in these programs. For the first time in this type of programs, regulators in the United States approved some fintech companies to have a role to play in the program by helping small businesses that may not have an established lending relationship with a large bank, community bank or credit union. Additionally, the fintech firms through automation and technology believe they will be able to process applications much more quickly.

This puts fintech firms, and particularly data-driven lenders in a spot they did not have before. This is the first economic crisis in which they will be able to demonstrate how beneficial these new business models can be for the economic recovery. (...)

Another consequence of the pandemic that has accelerated data-driven lending impact, are the creation of new partnerships between banks and fintech companies. Indeed, models are being re-evaluated to make them more flexible and more adaptive to the businesses. For example, some companies are working to promote their QR code contactless payment services, which allow SMEs to conduct sales while mitigating health risks due to COVID-19.[217] This transactional data will allow fintechs and other institutions with access to that transactional data to enrich their credit risk models, especially in a sector that lacks traditional finance information required to apply for a loan. Particularly in Mexico, fintechs are becoming a leading growth partner to SMEs through transactional data which helps understand the needs

[213] 'Coronavirus (COVID-19): SME Policy Responses' (n 211).
[214] Some media outlet reported that some banks could take two hours to collect this information and sometimes weeks to verify the information of applicants who were not existing lending customers. See Donna Fuscaldo, 'As COVID-19 Lenders, PayPal, Square, Other Fintechs Get To Prove They Can Do It Better Than Banks' (*Forbes*, 15 April 2020) <https://www.forbes.com/sites/donnafuscaldo/2020/04/15/as-covid-19-lenders-paypal-square-other-fintechs-get-to-prove-they-can-do-it-better-than-banks/> accessed 8 January 2021.
[215] For example, China's traditional banking sector. See Douglas W Arner and others, 'Digital Finance & The COVID-19 Crisis' [2020] University of Hong Kong Faculty of Law <https://papers.ssrn.com/abstract=3558889> accessed 7 January 2021.
[216] For instance, United States with the creation of the Paycheck Protection Program, which which helps businesses secure forgivable loans and keep workers employed. See 'Paycheck Protection Program' (*Small Business Administration*, 2020) <https://www.sba.gov/funding-programs/loans/coronavirus-relief-options/paycheck-protection-program> accessed 20 July 2020.
[217] See Celine Bteish and Marie-Sarah Chatain, 'COVID-19: Digital Finance Models to the Rescue of SMES in Latin America' (*SME Finance Forum*, 4 July 2020) <https://www.smefinanceforum.org/post/covid-19-digital-finance-models-to-the-rescue-of-smes-in-latin-america> accessed 8 January 2021.

and demands of clients.[218] Data is key because it also helps understand which sector and clients will recover the fastest. This in return, is important for fintech to prioritize loans provision.[219]

Finally, the data-driven finance evolution of the lending landscape is not only related to fintechs. Banks are also playing an important role. Through partnerships with associations that represent specific industry segments, banks in Asia are understanding the particular problems and needs of that sector to identify innovative products and services where they could play a meaningful role.[220] Through these partnerships, banks and fintechs are offering payment solutions for businesses that were not using e-commerce platforms.[221]

Financial Inclusion[222]

Lockdowns and social distancing are accelerating the digitization of many sectors, including financial services. Just as the SARS epidemic in 2003 expedited China's path in launching digital payments and e-commerce in the country,[223] some countries are taking steps to facilitate the massive use of digital financial services, especially digital payments. Digital payments are now a backbone to China's vibrant digital economy and its development highly influences data-driven initiatives.[224] Contactless payments to taxi drivers, vendors and even temples and beggars are possible through scanning a QR code. Payments for daily essentials, such as mobile phone bills, utilities, rent or internet fees, can all be made through mobile payments or online banking in China. Governments at all levels there also accept mobile payments as a payment method. Digital payments, in China, have almost become a public good and are definitely a key factor in data-driven finance.[225] Data and analytics is becoming the foundation of effective business decision making. In most countries digital payments services are evolving into digital

[218] Bteish and Chatain (n 217).

[219] Even though, it is important to note that not all jurisdictions have implemented this type of prudential regulatory requirements for fintechs.

[220] For example, DBS working with the Restaurant Association of Singapore, as the Food and Beverage (F&B) industry was losing 30-80% of revenues due to quarantine restrictions - yet their operating costs remained the same. Compounding those problems was the fact that established food delivery platforms were charging restaurants 30-33% commission on the total bill, thereby significantly narrowing profit margins for restaurants. To address this issue, DBS partnered with the government of Singapore and two homegrown fintech companies, Oddle and FirstCom, to roll out a Digital Relief Package for the F&B industry. Specifically, they enabled F&B businesses to set up an online food ordering site in just three days with much-reduced delivery rates. As a result, DBS enabled SMEs to quickly create additional online channels in order to increase revenue. See Jade Hachem and Gillette Conner, 'COVID-19 - A Catalyst for Digital Transformation in the SME Lending Ecosystem' (*SME Finance Forum*, 23 April 2020) <https://www.smefinanceforum.org/post/covid-19-a-catalyst-for-digital-transformation-in-the-sme-lending-ecosystem> accessed 8 January 2021.

[221] See Shivraj Rajendran, 'Bank Aims to Help F&B Clients Draw Online Customers' *The Straits Times* (26 March 2020) <https://www.straitstimes.com/business/bank-aims-to-help-fb-clients-draw-online-customers> accessed 8 January 2021.

[222] Header from original paper.

[223] See Yan Xiao and Martin Chorzempa, 'How Digital Payments Can Help Countries Cope with COVID-19, Other Pandemics: Lessons from China' (*World Economic Forum*, 6 May 2020) <https://www.weforum.org/agenda/2020/05/digital-payments-cash-and-covid-19-pandemics/> accessed 8 January 2021.

[224] See 'BigTech in Finance: Market Developments and Potential Financial Stability Implications' [2019] Financial Stability Board <https://www.fsb.org/wp-content/uploads/P091219-1.pdf>.

[225] See 'How Fintech Is Shaping China's Financial Services?' (Pricewaterhouse Coopers 2018) <https://www.pwccn.com/en/research-and-insights/how-fintech-is-shaping-china-financial-services.pdf>.

lending, as companies accumulate users' data and develop new ways to use it for creditworthiness analysis.[226]

Many countries[227] are replicating this model in similar ways and supporting this shift with measures such as lowering fees and increasing limits on mobile money transactions.[228] During the COVID-19 lockdowns, digital financial services are enabling governments to provide quick and secure financial support to people and businesses,[229] as demonstrated in Namibia, Peru, Colombia, Zambia, and Uganda.[230] In many of these jurisdictions, payment service providers were used to disburse government subsidies to people that did not use a digital financial channel before.[231]

This is expected to help mitigate the economic fallout and potentially strengthen the recovery. The pandemic shows that the trend towards greater digitalization of financial services is here to stay. (...)

Going digital and customer experience[232]

The pandemic has pushed financial institutions to significantly go digital. However, this transition to be a fully digital company, in most cases requires regulatory changes. Accordingly, the Financial Action Task Force (the FATF), issued a set of measures to combat illicit financing, and encouraged the use of the flexibility built into the FATF's risk-based approach to address some COVID-19 related challenges such as digital onboarding and simplified due diligence for Know Your Customer processes.[233] Regulation plays a critical role in enabling the transition to a digital environment. As mentioned, some countries have maintained more restrictive regulations on consumer data protection, especially when it comes to cloud acceptance and e- Know Your Customer and Anti-money Laundering practices. Dissimilar regulatory regimes have been extremely challenging for digital lenders which have tried to promptly implement a uniform action plan across various markets. The pandemic has driven regulators to re-think their approaches to facilitate even more the change into a digital experience.

Additionally, due to mobility restrictions of quarantines and lockdowns, financial institutions have been challenged to help address customer concerns in multiple channels such as online chats. Hence, digital banking, specifically "conversational banking" seems to have permanent uptrend in this period. Conversational platforms powered by Artificial Intelligence are increasing. The rise in the number of users and the dialogues in live chatbots have been reported by some technology companies. A company that partners with financial institutions to develop

---

[226] See Ulric Eriksson von Allmen and others, 'Digital Financial Inclusion in the Times of COVID-19' (*International Monetary Fund Blog*, 1 July 2020) <https://blogs.imf.org/2020/07/01/digital-financial-inclusion-in-the-times-of-covid-19/> accessed 8 January 2021.
[227] Mostly located in Africa, Asia and Latin America. See Allmen and others (n 226).
[228] Allmen and others (n 226).
[229] See Nana Yaa Boakye-Adjei, 'Covid-19: Boon and Bane for Digital Payments and Financial Inclusion' (2020) Financial Stability Institute Briefs Bank for International Settlements <https://www.bis.org/fsi/fsibriefs9.pdf>.
[230] See Allmen and others (n 226).
[231] See Nitish Narain and others, 'CICO Agents: The Under-Valued "First Responders"' (*Microsave Consulting*, 15 April 2020) <https://www.microsave.net/2020/04/15/cico-agents-the-under-valued-first-responders/> accessed 8 January 2021.
[232] Header from original paper.
[233] See 'Statement by the FATF President: COVID-19 and Measures to Combat Illicit Financing' (*Financial Action Task Force*, 1 April 2020) <https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html>.

chatbots in Turkey and the United States, reported that the number of users and messages has increased 5,4 and 3,9 times respectively in the banking chatbots since the outbreak of COVID-19.[234] The top asked topics have been loan application, credit payment delay, online banking password setting and request. (...)

Central Bank Digital Currencies[235]

The debate around the creation of Central Bank Digital Currencies was surprisingly accelerated by the pandemic in some jurisdictions, such as United States and China. Millions of U.S. taxpayers have waited for weeks for promised stimulus payments of up to $1,200 per person as a result of one of the measures taken to help people to navigate the COVID-19 crisis. While some received direct deposits in mid-April, those without bank accounts or a bank account on file with the Internal Revenue Service, who have not received a tax refund in recent years or who are married to an immigrant are still expecting that a check will arrive.

Supporters of digital dollars and central bank digital currencies say a digitized monetary system could solve the logistical question of how to quickly disburse large sums to many individuals with varying access to banking services.[236]

The Bank of China has recently completed the basic function development of a digital Yuan and it has moved one step closer to launch its CBDC during a middle of global recession. A number of Shenzhen-based private companies including Alibaba, Tencent, Huawei and China Merchants Bank have participated in the development of the digital currency. As central banks around the world are cutting interest rates to zero and taking aggressive action against the economic recession due to the coronavirus pandemic, China's central bank is accelerating its central bank digital currency plan and for some, turning these challenging times into an opportunity given that the digital asset is seen as the most convenient tool to translate a central bank's zero and negative interest rate policy into commercial banks.[237]

According to the Bank for International Settlements (BIS), irrespective of whether health concerns are justified or not, perceptions that cash could spread pathogens may change payment behaviour by users and firms.[238] In any case, and regardless of the motive behind it, digital payments are trending in the pandemic. However, the BIS raised some concerns about the distributional consequences of any move away from cash. If cash is not generally accepted as a means of payment, this could open a 'payments divide' between those with access to digital payments and those without. This in turn could have an especially severe impact on unbanked and non-digital consumers (generally the most vulnerable: with no access to digital infrastructure and elderly). (...)

However, [the digital transformation] also raises challenges and risks that regulators should adequately address. These risks and challenges are not minor. They mostly relate to financial

---

[234] See 'Covid-19 and Rise of Conversational Banking' (*CBOT*, 13 May 2020) <https://www.cbot.ai/covid-19-and-conversational-banking/> accessed 20 July 2020.
[235] Header from original paper.
[236] See Meena Thiruvengadam, 'How the COVID-19 Crisis Revived the Digital Dollar Debate' (*CoinDesk*, 8 May 2020) <https://www.coindesk.com/coronavirus-what-is-digital-dollar-cbdc-explainer> accessed 8 January 2021.
[237] See Ting Peng, 'Turning a Crisis Into an Opportunity, China Gets One Step Closer to CBDC' (*Cointelegraph*, 24 March 2020) <https://cointelegraph.com/news/turning-a-crisis-into-an-opportunity-china-getting-one-step-closer-to-cbdc> accessed 8 January 2021.
[238] See Raphael Auer, Giulio Cornelli and Jon Frost, 'Covid-19, Cash, and the Future of Payments' (2020) 3 Bank for International Settlements Bulletin <https://www.bis.org/publ/bisbull03.pdf>.

stability due to new systemically important players that could fall outside the regulatory perimeter,[239] cybersecurity, investor protection, consumer protection, competition, fairness, new and unexpected new forms of interconnectedness. The lack of interpretability or auditability of AI and machine learning methods could also become a macro-level risk for the financial sector. Similarly, a widespread use of opaque AI models may result in unintended consequences.[240] The challenges related to how to translate the discussion about high level principles of AI Governance is also important to mitigate some of these risks.[241]

Currently, regulators around the world, international setting bodies and academics discuss how to address those challenges what is the appropriate regulatory architecture to help shape the data revolution.[242] However, it is not an easy task for regulators to address all these challenges and promote financial innovation. While trying to strike the right balance, regulators face unavoidable conflicts between policy objectives.[243] Moreover, the data revolution of the financial services industry, as well as other innovations, exacerbate the trade-offs between different regulatory objectives. Financial services are unbundled because of these innovations, supply chains and financial intermediation are changing traditional forms and creating new levels of interconnectedness.[244] ***[Financial System paper]***

[239] For example, cloud services providers. See Nydia Remolina, 'Cloud Computing in Financial Services: Redefining Systemic Risk' SMU Centre for AI & Data Governance Research Paper (Forthcoming).

[240] 'BigTech in Finance: Market Developments and Potential Financial Stability Implications' (n 224).

[241] Some financial regulators are debating how to approach this discussion. For instance, the Monetary Authority of Singapore issued a set of principles to promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector. Now the regulatory authority is working closely with the tech and financial industries to translate these high level principles into specific recommendations applicable to some use data-driven applications in the financial sector. This initiative is called Veritas. The first phase will commence with the development of fairness metrics in credit risk scoring and customer marketing. See 'Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector' (Monetary Authority of Singapore) <https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf>; 'MAS Partners Financial Industry to Create Framework for Responsible Use of AI' (*Monetary Authority of Singapore*, 13 November 2019) <https://www.mas.gov.sg/news/media-releases/2019/mas-partners-financial-industry-to-create-framework-for-responsible-use-of-ai> accessed 8 January 2021.

[242] See Johannes Ehrentraud and others, 'Policy Responses to Fintech: A Cross-Country Overview' (2020) 23 FSI Insights on policy implementation <https://www.bis.org/fsi/publ/insights23.pdf> accessed 8 January 2021.

[243] See Chris Brummer and Yesha Yadav, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235.

[244] See Brummer and Yadav (n 243); Remolina (n 239); Nydia Remolina, 'Open Banking: Regulatory Challenges for a New Form of Financial Intermediation in a Data-Driven World' (2019) 2019/05 SMU Centre for AI & Data Governance <https://papers.ssrn.com/abstract=3475019> accessed 8 January 2021.

4. Regulatory aims and focus

With these challenges laid out, this chapter proceeds with some recommendations on how States and other interested stakeholders can work towards eliminating and tackling the above-mentioned issues. The suggestions posited here invite a consideration of the functional and important role of ethics, law, and State institutions in today's pandemic governance handling and strategies.

A note to readers who are interested in this chapter: A considerable portion of the excerpts cited in this section were derived from the *Covid Regulation paper* published by Findlay and Remolina. Various sections of the original paper were extracted and cited in this order to promote the readability of the compendium. Readers are strongly encouraged to read the original paper in full for a better appreciation of the context in which these recommendations were proposed.

4.1 Eliminate discrimination

Vulnerable groups may be discriminated against as a result of state (or private-sector) imposed control measures, or through their exclusion or ostracization from the relevant protection measures or social assistance schemes. Discrimination may arise from the application and employment of discriminatory tech measures, or through the use and repurposing of tech-produced data that perpetrates bias, stigma, and other negative social/economic consequences against these marginalised populations. The excerpts below seek to provide some guidance to authorities in their consideration of how to ameliorate discriminatory consequences in order to produce more equitable social and healthcare outcomes for vulnerable persons.

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. (...)

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. ***[Covid Regulation paper]***

4.2 Promote transparency, explainability, and digital accessibility

As mentioned above, the way to produce better regulatory strategies and policy intervention is to ensure adherence to key ethical principles such as the principle of transparency. The papers make clear three areas where transparency is critically instrumental: First, transparency in decision-making including the way data is collected and utilised by the state (or other relevant stakeholders). Second, transparency in communication including the *type* of information, *how* such information is being communicated, and *when* the public receives crucial information that are relevant to them is significant. Finally, the principle of transparency is also important (and linked to accountability) because of its interest and receptivity in the design of an appropriate monitoring/scrutiny function that stifles arbitrary powers and measures.

Closely linked to the principle of transparency is the principle of explainability. States' adherence to the ethical principle of explainability would similarly benefit pandemic governance approaches by ensuring that information communicated is understandable by the public at large. Comprehensibility is important for the purposes of societal participation and engagement. The excerpts below highlight the significance of the

principle, as well as suggest practical steps to take in order to achieve greater community comprehension, and understanding. Wee and Findlay, in addition, examine the Singapore TraceTogether use case and outline how the principles of transparency and explainability can be improved in the city-state.

Finally, while the rapid rise and reliance on technology has shown to be of considerable benefit in controlling the spread of the pandemic, it is concerning that access to technology is not equal across the board. The excerpt below explores the consequences of this lack of accessibility, where marginalised population segments who do not have access to the necessary technology are excluded from important safeguards proffered to wider society.

Transparency

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.[245] 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 individual liberties are mandated constitutionally.[246] (...)

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. ***[Covid Regulation paper]***

~

[...] Corona-Warn-App,[247] has won much praise for its transparency.[248] The app was developed through an open-source collaboration between SAP and Deutsche Telekom, based on the Exposure Notification Framework provided by Apple and Google. Further, the source code and data protection impact assessment are also made readily available to scrutiny.[249] Data is both collected and encrypted,[250] and the tech is considered less invasive than other apps that access and analyse location data and GPS locations. The German Federal Commissioner for Data

[245] Ienca and Vayena (n 78).
[246] Will Knight, 'The Value and Ethics of Using Phone Data to Monitor Covid-19' [2020] *Wired* <https://www.wired.com/story/value-ethics-using-phone-data-monitor-covid-19/> accessed 2 April 2020.
[247] The Corona-Warn-App was launched on 16 June 2020. See 'Germany Launches Coronavirus App as EU Eyes Travel Revival' *Reuters* (16 June 2020) <https://www.reuters.com/article/us-health-coronavirus-germany-app-idUSKBN23N160> accessed 1 September 2020.
[248] Deutsche Welle (www.dw.com), 'German COVID-19 Warning App Wins on User Privacy | DW | 15.06.2020' (*DW.COM*) <https://www.dw.com/en/german-covid-19-warning-app-wins-on-user-privacy/a-53808888> accessed 5 August 2020.
[249] 'Internetauftritt Des Bundesbeauftragten Für Den Datenschutz Und Die Informationsfreiheit - Press Office - Sufficient Data Protection in the Corona Warning App' <https://www.bfdi.bund.de/EN/Home/Press_Release/2020/12_Corona-Warning-App.html;jsessionid=2F61428EAA12AFE817AE3703F2A6BF8A.1_cid354> accessed 5 August 2020.
[250] Janosch Delcker, 'Privacy-Savvy Germany Launches Coronavirus Contact-Tracing App' (*POLITICO*, 16 June 2020) <https://www.politico.eu/article/germany-privacy-coronavirus-contact-tracing-app/> accessed 5 August 2020.

Protection and Freedom of Information has also commented that from a data protection perspective, there is no argument against installation as the stated that the level of data security is sufficient.[251]

Taking a hybrid approach, Italy's contact tracing app, Immuni,[252] is also based on the Apple and Google framework, and sees the adoption of a semi-centralised system, similar to Singapore's TraceTogether. The system is decentralised and collects no personal data, but a patient who has tested positive can choose to upload their results (with a special key) and share with the government-run central server.[253] ***[Disquiet paper]***

~

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[254] the data subject should have the opportunity for timely and fair challenging of these conclusions and limits.m[255] Moreover, explainability is a guiding principle within most if not all the ethical data use guidelines that companies and governments have published.[256] 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. (...)

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

[251] 'Internetauftritt Des Bundesbeauftragten Für Den Datenschutz Und Die Informationsfreiheit - Press Office - Sufficient Data Protection in the Corona Warning App' (n 249).
[252] Immuni was launched on 1 June 2020, which reported over 500,000 downloads within the first 24 hours after its launch. See 'Italy Launches Immuni Contact-Tracing App: Here's What You Need to Know' (5 June 2020) <https://www.thelocal.it/20200605/italy-to-begin-testing-immuni-contact-tracing-app-in-four-regions> accessed 1 September 2020.
[253] Hadas Gold Business, 'Tracking Apps Were Supposed to Help Beat the Pandemic. What Happened to Them?' (*CNN*) <https://www.cnn.com/2020/06/05/tech/coronavirus-tracking-apps/index.html> accessed 5 August 2020.
[254] For example in Europe under the General Data Protection Regulation.
[255] Guariglia and Schwartz (n 71).
[256] Nagy and Fjeld (n 133).

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. ***[Covid Regulation paper]***

~

In efforts to raise transparency of the app design and use, Singapore's Government Technology Agency has released a comprehensive white paper outlining the data which TraceTogether is collecting, and the trust-by-design premise that the app is built upon to safeguard privacy.[257] While the white paper was laudable in its intention to offer insights into technical and policy considerations that the developers dealt with in order to create the TraceTogether protocols, we suggest that more action could have been taken by the state to share the document with TraceTogether users from the app's launch in a simple and accessible form. It is notable that the white paper is not readily available via the TraceTogether app, nor has it been widely communicated through the government's social media channels. This failure of public communications may have exacerbated the app's inaccessibility to users, as demonstrated by reviewers in the app stores repeating queries which were pre-empted and already addressed in the white paper. Moreover, the content of the white paper is not easily understood by all users of the app, as it requires the reader to possess certain technical appreciation of the software to digest the information contained within it.

In addition to the white paper, GovTech has also released a shorter piece on its website, "9 geeky myth-busting facts you need to know about TraceTogether",[258] to address commonly misunderstood aspects of the app in a more accessible manner. These 'facts' include express clarifications that the app is not used to track or spy on citizens whereabouts, and that consent to the in-app functions of the phone does not equate to providing the government with unlimited access to all of the user's personal and phone data. Unfortunately, much like the white paper, this released statement is not easily located within the app's interface (even within in its help section), or on its related website. These efforts, albeit commendable, happen only after the technology has been released. Therefore such explanations and justifications of the technology has been described as "mere performances of public participation", reinforcing the top-down practices of the state regarding citizen inclusion.[259] ***[Disquiet paper]***

~

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 older 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. ***[Covid Regulation paper]***

---

[257] Jason Bay and others, 'BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing across Borders' 9.
[258] '9 Geeky Myth-Busting Facts You Need to Know about TraceTogether' (n 92).
[259] Monamie Bhadra Haines and Stevens, 'Governed by Tech: Citizens and the Making of the Smart Nation' (*Academia | SG*, 14 October 2020) <https://www.academia.sg/academic-views/governed-by-tech-citizens-and-the-making-of-the-smart-nation/> accessed 21 October 2020.

4.3 Ensure good data governance and proper data management practices

Good data governance is especially crucial for pandemic crisis management to generate/promote citizens' trust and preserve political reputations. As we have explored in the sections above, extraordinary quantities of data are continually collected, analysed, and put to use by various states and corporations for a host of pandemic containment purposes. Data subjects rely on these agents (who are in a position of authority and power) to properly store, manage, study, and share their information. The included excerpts explain *why* powers held by States and private corporations must be exercised responsibly and *how* the relevant stakeholders can go about doing so.

There is also a need to acknowledge that self-regulatory privacy-by-design frameworks are inadequate for promoting good data governance as it goes only as far as the agency culturally and commercially accepts it. The excerpts below build on this to emphasise the need for the installation of an independent protection agency in the personal data protection pyramid.

To promote good data governance practices, it has been proposed that States should also implement sunset clause provisions into COVID-19 emergency legislations related to personal data-harvesting and data sharing measures. To avoid ineffective reviews such as "rubber-stamp" re-approvals of sunset clauses, data subjects should be empowered to participate in the reviews of these policy extensions.

Finally, the heavy reliance on technology-driven solutions for contact tracing and surveillance has led to increasing concerns over the safety and security of data subjects and healthcare systems. The excerpts below seek to illustrate the importance of safeguarding and enhancing cybersecurity practices and urges governments to rethink their data security priorities and other health data processing initiatives.

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.[260] 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.[261] To avoid any tragic repeat of this resistance in future crises, and to learn

[260] 'Lack of COVID-19 Preparedness in Line with Previous Findings, Economists Find' (*ScienceDaily*, 14 May 2020) <https://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.

[261] 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-

from mistakes around the control strategy communication, if communities could be 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 good governance and Data justice[262]

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 extraordinary 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. ***[Covid Regulation paper]***

Privacy by design is not enough[263]

poll-finds/> accessed 20 May 2020; Carlos Cantú and others, 'On Health and Privacy: Technology to Combat the Pandemic' (2020) 17 BIS Bulletin <https://www.bis.org/publ/bisbull17.pdf> accessed 20 May 2020.

[262] Header from original paper.

[263] Header from original paper.

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.[264] However, privacy by design is actually embedded within the processes of most companies who have recently come under scrutiny for suspect privacy practices.[265] 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.[266] 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 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. ***[Covid Regulation paper]***

Expiration of the use of data[267]

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.

---

[264] 'Tracking and Tracing COVID: Protecting Privacy and Data While Using Apps and Biometrics' (*Organisation for Economic Co-operation and Development (OECD)*, 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.

[265] Ira Rubinstein and Nathan Good, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' (2012) 28 Berkeley Technology Law Journal 1333.

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

[267] Header from original paper.

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.[268]

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, 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.[269]

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.[270] 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.[271] 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

[268] 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.
[269] Sofia Ranchordás, 'Sunset Clauses and Experimental Regulations: Blessing or Curse for Legal Certainty?' (2015) 36 Statute Law Review 28; Ittai Bar-Siman-Tov, 'Temporary Legislation, Better Regulation, and Experimentalist Governance: An Empirical Study' (2018) 12 Regulation & Governance 192.
[270] Ranchordás (n 269).
[271] Christian Bjornskov and Stefan Voigt, 'The State of Emergency Virus' (*Verfassungsblog*, 19 April 2020) <https://verfassungsblog.de/the-state-of-emergency-virus/> accessed 15 May 2020.

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.[272] 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.[273]

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 allows for indefinite detention of non-national terrorist suspects. The Act was reviewed in 2003, but with little scrutiny.[274]

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. ***[Covid Regulation paper]***

Cybersecurity[275]

Ransomware attacks on hospitals and health systems have continued during the pandemic, raising key cybersecurity considerations about infrastructure disruptions.[276] 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.[277]

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

---

[272] 'Coronavirus Act 2020' (*legislation.gov.uk*) <https://www.legislation.gov.uk/ukpga/2020/7/contents> accessed 15 May 2020.

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

[274] Molloy (n 273); 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 (Springer Science & Business Media 2011).

[275] Header from original paper.

[276] 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.

[277] 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.

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.[278] 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.[279] 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.

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. ***[Covid Regulation paper]***

4.4 Respect individual rights

The current health crisis and its narrative should not be drawn on to justify the State's unlimited interference with individuals' rights. States should continue to safeguard personal rights and liberties and account for any deviations in the traditional rights framework. Personal rights should not be disregarded in its entirety but must be balanced against other public goods such as the right to public health. Further, to ensure that pandemic containment responses are effective, appropriate, and fair, it is also important for authorities to have in mind an appropriate expiration date for their retirement (when measures are seen as no longer necessary or fit for purpose) and to see to the restoration of rights that were initially constrained.

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 individual rights for communal benefit. So, stay-home orders and social distancing are seen inevitably as compromising liberties of association and movement. 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. (...)

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.[280] 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.

[278] 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.
[279] Lynn (n 278).
[280] The European Data Protection Board coincides with this approach. See Antoine Olbrechts, '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/outros/statement-processing-personal-data-context-covid-19-outbreak_en> accessed 7 April 2020.

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. (...)

Timetables for expiration at this stage are difficult to set but the importance of the policy objective can be presently agreed. (...)

[...] if the surveillance mechanisms are to remain active for prevention purposes, it is important to regularly revisit the initial terms of the emergency exercise, and, in particular, its limited and contained health objectives. Simply to have this data as a stalking horse for all kinds of other social control preferences denies the initial emergency justifications and endangers their acceptance if they become a common call for social control and many other forms. ***[Covid Regulation paper]***

~

These surveillance programmes are based on reasons related to public interest in controlling the spread of the COVID-19 pandemic. Those reasons require clear public enunciation. As the scale and severity of the COVID-19 pandemic rises to the level of a global public health threat[281] justifying restrictions on certain rights,[282] then causal relations between threat, control policy and intended outcomes require monitoring. Indeed, under the International Covenant on Economic, Social and Cultural Rights, which most countries have adopted, individuals have the right to "the highest attainable standard of physical and mental health." Governments are obligated to take effective steps for the "prevention, treatment and control of epidemic, endemic, occupational and other diseases."[283] 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. ***[Ethics paper]***

---

[281] 'Coronavirus Disease (COVID-19) – World Health Organization' <https://www.who.int/emergencies/diseases/novel-coronavirus-2019> accessed 6 January 2021.

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

[283] See 'International Covenant on Economic, Social and Cultural Rights' (*United Nations Human Rights, Office of the High Commissioner*) <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx> accessed 20 May 2020. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 3 January 1976, in accordance with article 27. Available at: https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx
Additionally, the United Nations Committee on Economic, Social and Cultural Rights, which monitors state compliance with the covenant, has stated that: "The right to health is closely related to and dependent upon the realization of other human rights, as contained in the International Bill of Rights, including the rights to food, housing, work, education, human dignity, life, non-discrimination, equality, the prohibition against torture, privacy, access to information, and the freedoms of association, assembly and movement. These and other rights and freedoms address integral components of the right to health." See 'CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)' [2000] United Nations: Office of the Human Rights Commissioner <https://www.refworld.org/pdfid/4538838d0.pdf> accessed 27 April 2020.

4.5 Secure Data integrity and eradicate bias

The increased access to and sharing of data in this health crisis makes it all the more important to ensure that data integrity is properly safeguarded. Data integrity involves ensuring that data used in this health crisis is genuine, fit for purpose, and accurate.

The eradication of bias is also important for the purpose of securing data integrity. The excerpts reveal how bias in automated data systems informing governments' COVID-19 responses can have severe consequences, such as leaving out entire populations, misrepresenting others, and leading to ineffective containment efforts and deployment of healthcare resources.

In the excerpts below, we highlight recommendations and directions on how the two targets can be achieved.

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,[284] or to play a part in containing the virus, counter-narratives have emerged which rehearse reservations about the consequences of such mass data sharing.[285] 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. (...)

It is important to ensure that data is genuine and fit for the declared purpose, particularly if that emergency purpose is 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.[286]

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).

---

[284] Sunstein (n 83).
[285] Urs (n 84).
[286] Kevin H Govern and John Winn, 'Data Integrity Preservation and Identity Theft Prevention: Operational and Strategic Imperatives to Enhance Shareholder and Consumer Value' [2012] Risk Management and Corporate Governance, Abol Jalilvand and A. G. Malliaris, ed., Routledge <https://papers.ssrn.com/abstract=2128834> accessed 6 January 2021.

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 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.[287] In keeping with the specific responsibilities for promoters they should propose KPIs overseen by the CPDC. ***[Covid Regulation paper]***

~

Eradicate bias

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.[288] Against this experience, it is necessary to ensure that any automated data systems used to contain COVID-19 do not erroneously identify members of specific demographic groups as particularly susceptible to infection.[289] Insufficient or ineffective de-identification and biases in datasets can become major causes of distrust in public-health services. (...)

---

[287] 'Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19: Common EU Toolbox for Member States' (2020) Version 1.0 European Commission, eHealth Network 1.

[288] Demonising outsiders has proved to be common during pandemics. In the United States, existing anti-Asian prejudice fed on the disease's Chinese origin. When lumber yard proprietor Wong Chut King died of suspected plague in San Francisco in 1900, the authorities forcibly quarantined Chinatown, roping it off and surrounding it with police. Restrictions targeted ethnicity, not the likelihood of contact with the disease – white people were allowed to leave while Chinese people were contained. During the 1890s, a typhus outbreak on an immigrant ship led to the detention of 1,200 Russian Jews, and well into the 20th century new arrivals at Ellis Island faced segregation based on suspicion of infection. See Caroline Rance, 'Demonising Outsiders and Stoking Racial Tensions: The Dark History of Quarantine Practices' [2020] *HistoryExtra* <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 Hannah Marcus, 'What the Plague Can Teach Us About the Coronavirus' *The New York Times* (1 March 2020) <https://www.nytimes.com/2020/03/01/opinion/coronavirus-italy.html> accessed 27 April 2020.

[289] Guariglia and Schwartz (n 71).

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. (...)

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.[290] 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.[291] 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. ***[Covid Regulation paper]***

4.6 Oversee private sector data sharing

During this pandemic, several states have utilised technology offered by private corporations, such as the Google-Apple's Exposure Notification system in the

[290] 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 Tools 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 3rd Quarter 2020' (*Statista*) <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> accessed 20 May 2020.

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

implementation and enforcement of contact tracing measures. The private sector's capacity to acquire vast amounts of data collected, especially sensitive personal information, ought to be scrutinised. The massive quantity of data amassed has brought about significant privacy concerns, relating to how much information corporations have over the data subjects, as well as how these collected data are being stored. The following paragraphs discuss the value of having these corporations adopt privacy legislative practices, such as "information fiduciary" rules.

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 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.[292]

Accordingly, some have proposed adapting these venerable fiduciary rules to apply to online companies that collect personal data from their customers.[293] New laws would define such companies as "information fiduciaries."[294] 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.[295]

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

---

[292] Sylvie Delacroix and Neil Lawrence, 'Bottom-Up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance' (2019) 9 International Data Privacy Law 236.
[293] 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> accessed 6 January 2021; Neil Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stanford Technology Law Review 431.
[294] Gebhart (n 268).
[295] Delacroix and Lawrence (n 292).

offers of surveillance/tracing technologies available in a specific jurisdiction. ***[Covid Regulation paper]***

4.7 Promote ethical surveillance

As more States stress on the need to utilise surveillance technologies as part of their pandemic control response, this has brought along an array of concerns relating to the mandatory and omniscient nature of surveillance that a data subject cannot consent to, or escape from, all the while questioning the need for highly invasive personal data to be collected. The excerpts below bridge the debate between individual privacy and public safety, and propose a mechanism in which surveillance models can co-exist with existing privacy protections.

Related to this subject is the need to prevent anxiety governance. The climate of anxiety and polarisation exacerbated by the pandemic makes it all the more important to guard against anxiety-inducing reporting by both social and conventional news platform providers. The excerpts below offer two regulatory obligations that policymakers and news platform providers should meet to reduce citizens' anxiety.

State sector surveillance[296]

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.[297] 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.[298] 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.[299]

---

[296] Header from original paper.

[297] Amanda Meade, 'Australian Coronavirus Contact Tracing App Voluntary and with "No Hidden Agenda", Minister Says' *The Guardian* (18 April 2020) <http://www.theguardian.com/technology/2020/apr/18/australian-coronavirus-contact-tracing-app-voluntary-and-with-no-hidden-agenda-minister-says> accessed 20 May 2020.

[298] 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.

[299] Joseph Duball, 'Centralized vs. Decentralized: EU's Contact Tracing Privacy Conundrum' *International Association of Privacy Professionals (IAPP)* (28 April 2020) <https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum/> accessed 20 May 2020.

The starting point for the European Data Protection Board Guidance for COVID-19[300] 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. (...)

Anxiety Reduction[301]

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. 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 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.[302] (...)

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).[303] Second is the

---

[300] 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' [2020] European Data Protection Board <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf>.

[301] Header from original paper.

[302] 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.

[303] 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

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. ***[Covid Regulation paper]***

4.8 Preserve anonymity and privacy

In efforts to safeguard against concerns surrounding privacy invasions and breaches, researchers have repeatedly emphasised the need to anonymise identifiable personal information. While this is beneficial in theory, it is practically impossible to do so in practice. The section below details the issues surrounding preserving anonymity in a surveillance-infused climate, and the need for relevant stakeholders to exercise greater data management practices.

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.[304] A study from 2013 found that researchers could especially characterize 50% of people using only two randomly chosen time and location data points.[305] 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?[306] 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.[307] 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 personal data management practices in the fight against COVID-

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)

[304] 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.

[305] Yves-Alexandre de Montjoye and others, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' (2013) 3 Scientific Reports 1376.

[306] Hoffman-Andrews and Crocker (n 304).

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

19.[308] 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, 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.[309] 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.[310] Use-case evaluations on particular balancing considerations (protection of privacy and protection of public safety) would come within the independent agency's arbitration function. ***[Covid Regulation paper]***

[308] Hoffman-Andrews and Crocker (n 304).
[309] Hoffman-Andrews and Crocker (n 304).
[310] Hoffman-Andrews and Crocker (n 304).

5. Improving pandemic handling approaches

This chapter stresses the importance of modifying our current approaches to pandemic governance by introducing the need for better regulatory strategies and policy intervention. The excerpts below synthesise chapter 4's aims by focusing on three normative foundations that regulatory exercises should include: the avoidance of discrimination, the need to comply with ethical and principled design (while recognising that ethics as a standalone is insufficient), and the requirement for authorities' to commit to citizen inclusion and engagement. On the subject of what counts as strong pandemic governance, we also found it pertinent to highlight the significant role of the rule of law in helping to achieve greater public trust and State legitimacy. By enhancing the legitimacy of the State, there is a higher likelihood that citizens are more likely than not to comply with the State's pandemic containment measures thereby guaranteeing its overall success in curbing the spread of the virus.

5.1 Recognising that the language of ethics as a standalone is inadequate

It is increasingly clear that institutions have overrelied on the language of ethics (as a standalone) in determining and guiding State pandemic responses. This overreliance on ethical language has contributed to a legitimacy crisis because its self-governing framework is seldom adhered to in practice. The language of ethics may also be criticized for its lack of citizen engagement, participation, and actionability in the form of rights and remedies when ethical principles are breached. Other problems arising from relying on ethics as a regulatory framework include a lack of universal agreement on its guiding principles, it often has vague, open-ended definitions and issues with implementing/translating principles into practice.

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. ***[Covid Regulation paper]***

~

The power differentials which weigh heavily on the attribution and distribution of ethical responsibility across the AI ecosystem[311] mean that a simple and singular reliance on a principled self-regulatory frame is unconvincing and naïve. In any measure, community disquiet over the rights and integrity challenges posed by AI-assisted surveillance technology and resultant mass data sharing in current pandemic responses makes clear that resorting to ethics discourse to reverse the resistance that accompanies these control strategies will not always produce a sufficiently compliant social context for their successful operation. (...)

Simply put the argument recounts a growing dissatisfaction with ethics and principled design as either the single or primary self-regulatory regime ensuring responsible data use and trustworthy AI. From this foundation it proposes rule of law compliance as a parallel and

[311] Findlay and Seah (n 137).

supportive normative and operational direction to address the deficiencies likely in any over-reliance on ethics regulation. In expressions of resistance to COVID responses there has been little evidence of any prevailing confidence that assertions about ethical reflection answer the deeply felt and differentially identified reservations regarding surveillance and data usage in pandemic responses. (...)

This section summarises the main concerns emerging around ethical regulatory paradigms when applied to AI development and deployment, and the use of big data. Reduced to its essentials the critique advances on two fronts:

- that ethical principles as currently advanced by the AI and big data industry are elitist and insufficiently particular to form clear, strong and universal regulatory requirements, and
- that ethical attribution and distribution are not sufficient across the AI ecosystem due to the prioritising of organisational, commercial and professional counter-messages.

Over-representation of Industry Actors[312]

Private companies like Google, Microsoft, IBM and Tencent have taken the lead in publishing their own ethics documents and principles.[313] While it is unsurprising that companies at the forefront of AI development want to have a hand in shaping the debates around the very technologies they are building and marketing, it would be naive to expect that they will abide by voluntary standards in the face of market pressures and growth imperatives.[314] The murky overlap between developer and self-regulator demand an evaluation of likely contradictions in incentives that work against the regulatory mission.. The emergent critique in recent years has highlighted the hypocrisy of 'ethics washing', where industry players able to hide behind the promotion and marketing of *Ethical AI* as a form of principled self-regulation, which then functions as an alternative to legislation and other harder-edged regulatory intervention.[315] In addition, Hagendorff has also highlighted the risk of big tech influencing research through increasing public-private partnerships and industry-funded AI research operations, thereby posing the risk of a "gradual buyout of research institutes."[316]

Missing voices and issues from the debate[317]

While ethical principles abound in the AI self-regulatory discourse, some scholars have increasingly highlighted to the narrowness of their advocacy, where both problems and solutions said to be addressed through ethics reflect the privileged voices of a minority. Hagendorff (2020), emphasise the gendered division in the drafting of ethics principles:

> …the "male way" of thinking about ethical problems is reflected in almost all ethical guidelines by way of mentioning aspects such as accountability, privacy, or fairness. In contrast, almost no guideline talks about AI in contexts of care, nurture, help, welfare, social responsibility or ecological networks.[318]

[312] Header from original paper.
[313] Anna Jobin, Marcello Ienca and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1 Nature Machine Intelligence 389.
[314] Thilo Hagendorff, 'The Ethics of AI Ethics: An Evaluation of Guidelines' (2020) 30 Minds and Machines 99.
[315] Hagendorff (n 314).
[316] Hagendorff (n 314).
[317] Header from original paper.
[318] Hagendorff (n 314) 103.

The review of various principle statements internationally by Jobin, Ienca, and Vayena[319] also revealed an under-representation of input from regions such as Africa, South and Central America and Central Asia. As they see it, "more economically developed countries are shaping this debate more than others, which raises concerns about neglecting local knowledge, cultural pluralism and the demands of global fairness."

This lack of diversity in the discourse advocating ethical AI development and use risks the replication of older forms of power hierarchies through a North world dominant treatment. As Lee points out;

> [u]nless [developing economies] wish to plunge their people into poverty, they will be forced to negotiate with whichever country supplies most of their A.I. software — China or the United States — to essentially become that country's economic dependent, taking in welfare subsidies in exchange for letting the "parent" nation's A.I. companies continue to profit from the dependent country's users.[320]

Other important issues are similarly either missing or muted in the ethics self-regulatory discourse. These range from issues social responsibility and care, as mentioned above, to questions around the political abuse of AI software such as automated propaganda, bots, fake news, and deep fakes; on to the social and ecological costs of building AI systems, such as lithium mining, the exploitation of rare earth minerals, and the employment of "ghost workers" for data labelling and content moderation.[321]

Gaps in shifting from principles to practice[322]

Despite these reservations, and more general concerns about ever effectively operationalising such a smattering of general values and principles, there is continued activity within the AI and data management industries to translate at least some of these principles into practice. Aligned with this dynamic, most national AI strategies still revolve around a self-regulatory ethics core. As Hagendorff emphasises, accountability, privacy, or fairness appear in about 80% of all available guidelines and seem to be providing the "minimal requirements for building and using an "ethically sound" AI system." Much technical effort has been concentrated on materialising these principles, like IBM's "AI Fairness 360" toolkit and Google's "What-If Tool".

Even with a determination to operationalise the ethical use and development of AI within production teams, research suggests an increasing divide between the availability of ethics decision-making tools and their real-life application.[323] This normative/operational dissonance may be explained by the following challenges across the AI ecosystem:

---

[319] Jobin, Ienca and Vayena (n 313) 396.
[320] Kai-Fu Lee, 'The Real Threat of Artificial Intelligence' *The New York Times* (24 June 2017) <https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html> accessed 8 January 2021.
[321] Hagendorff (n 314); Mary L Gray and Suri Siddharth, *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass* (Houghton Mifflin Harcourt 2019); Sarah T Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (Yale University Press 2019) <https://doi.org/10.2307/j.ctvhrcz0v>; Kate Crawford and Vladan Joler, 'Anatomy of an AI System' (*Anatomy of an AI System*, 2018) <http://www.anatomyof.ai> accessed 8 January 2021.
[322] Header from original paper.
[323] Jessica Morley and others, 'From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices' (2020) 26 Science and Engineering Ethics 2141;

Uncertainty over the distribution of responsibility[324]

Who should take responsibility for thinking about the ethical implications of technology and the implementation of these ethics tools? How should responsibility be attributed and distributed across the AI ecosystem?[325] As Orr and Davis write,

> Technical systems pass through multiple hands over the trajectory of conception, design, implementation, and use. Myriad actors and organisations come in contact with a given AI product, and each has formative effects upon it. It remains unclear who the stewards of these technologies are, and where the burden of social responsibility lies.[326]

Similarly, Schiff et al.[327] have called this "the many hands problem", where the distribution expertise required to build and market AI product leads to fundamentally different areas of operational focus, wherein some priorities are not aligned with the promotion of ethical values. For example, technically trained engineers may emphasise the quality and safety of their products and ignore the wider social implications of their output while business managers prioritise fiduciary responsibilities and profit in terms contract obligations. On the other end of the spectrum, social scientists and ethicists who are the most interested in addressing principled design may be stuck in advisory capacities without sufficient operational resources or organisational capacity and institutional power to require functional/capacity changes in production teams to reflect ethical attribution.

Uncertainty over and difficulty in assessing the impact of AI/ML models on individuals and society[328]

Few ethics tools currently provide meaningful ways of assessing the impact/implications of using machine learning or an algorithm on individuals, their community, and society as a whole.[329] On site research has revealed that engineers tend to be more attuned to immediate and physical harms rather than broader evils such as social, emotional, or economic damage. Nonetheless, understanding risks posed by AI/ML models "requires looking well beyond a narrow set of topics such as bias, transparency, privacy, or safety and treating them as independent issues. Instead, the full range of topics and their complex interdependencies needs to be understood… such a task can be enormously difficult".[330]

A disjunct between the availability of tools and the capacity of AI practitioners to affect change[331]

Ville Vakkuri and others, 'Ethically Aligned Design of Autonomous Systems: Industry Viewpoint and an Empirical Study' [2019] arXiv preprint arXiv:1906.07946 <https://arxiv.org/pdf/1906.07946.pdf> accessed 8 January 2021; Daniel Schiff and others, 'Principles to Practices for Responsible AI: Closing the Gap' [2020] arXiv:2006.04707 [cs] <http://arxiv.org/abs/2006.04707> accessed 12 July 2020; Kenneth Holstein and others, 'Improving Fairness in Machine Learning Systems: What Do Industry Practitioners Need?' [2019] Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems 1.

[324] Header from original paper.

[325] For an answer to attribution and distribution see Findlay and Seah (n 137).

[326] Will Orr and Jenny L Davis, 'Attributions of Ethical Responsibility by Artificial Intelligence Practitioners' (2020) 23 Information, Communication & Society 719.

[327] Schiff and others (n 323).

[328] Header from original paper.

[329] Morley and others (n 323).

[330] Schiff and others (n 323).

[331] Header from original paper.

Finally, the current dissonance between the recognition of ethical responsibilities and their application in practice is due to the heavy reliance on the voluntary and conscious compliance by AI practitioners embedded within the essential technical expertise governing their models. Yet this group is often constrained in their decision-making capacities by commercial or organisational externalities that usually take priority, such as managerial norms and client mandates.[332] In highly competitive commercial and technological environments structured by comparatively pressing imperatives driving the "AI race",[333] the difficulty of measuring the success or failures of available decision-making constituents for addressing ethical issues means that;

> …there is no clear problem statement (and therefore now clear business cast) that the ML community can use to justify time and financial investment in developing much-needed tools and techniques that truly enable pro-ethical design. [334]

In summary, the problems with the current *ethical AI* debate are these:

- A minority of voices are shaping the debate's trajectory at the expense of a plurality of experiences, values, and norms.
- while the shift towards operationalisation does address the conceptual vagueness of AI principles[335] it also has the effect of placing too many expectations on individuals to change the resist of problematic and harmful AI deployments. These individuals, while well-positioned to influence operational outcomes with their technical expertise of data processing and model development, are both typically untrained to recognise the larger societal implications of their work and constrained in their decision-making capacities to allocate more time and resources to addressing ethical considerations.
- Can a solution be found for this uptake dilemma via a refinement of principled frameworks through the more focused application of micro ethics[336] or virtue ethics[337] to achieve the more equitable and just development and deployment of AI/ML systems?

On the final contention, D'Ignazio and Klein[338] demand a move away from the language of ethics entirely. They suggest that *ethics* remains insufficient as an AI regulatory paradigm because it continues to assume that the source of AI risks and challenges (perceived and actual) lies within individuals and the technical systems they create and maintain, thereby failing to "acknowledge structural power differentials and work towards dismantling them".[339] Accepting this is the case, then the soft law approach behind AI ethics remains inadequate to prompt a deeper engagement with entrenched market and machine assumptions motivating the advance of AI or to recognise and take account of shifting perceptions and norms in society,

[332] Orr and Davis (n 326).
[333] Hagendorff (n 314).
[334] Morley and others (n 323).
[335] Ben Green, 'Data Science as Political Action: Grounding Data Science in a Politics of Justice' [2018] arXiv:1811.03435 [cs] <http://arxiv.org/abs/1811.03435> accessed 17 July 2020; Jobin, Ienca and Vayena (n 313).
[336] Hagendorff (n 314).
[337] Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting* (Oxford University Press 2018).
[338] Catherine D'Ignazio and Lauren F Klein, *Data Feminism* (The MIT Press 2020).
[339] D'Ignazio and Klein (n 338) 60.

much less the much more complex "global systems of racial capitalism, class inequality, and heteronormative patriarchy, rooted in colonial history".[340] ***[ROL paper]***

5.2 Rethinking the rights discourse

As identified by the papers below, one of the main issues with overreliance on the language of rights as a framework for best practice is that its regulatory priority and appetite is inconsistent across different political, economic, and social contexts. Apart from the lack of universal purchase, the papers also note that the rights discourse is problematic (as with the language of ethics) because of similar issues relating to actionability and enforceability.

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.[341] This debate has raised protective options such as algorithm audits, data protection commissions, and independent recurrent evaluation.[342] 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.[343] 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)[344] However, in countries such as the

---

[340] Shakir Mohamed, Marie-Therese Png and William Isaac, 'Decolonial AI: Decolonial Theory as Sociotechnical Foresight in Artificial Intelligence' (2020) 33 Philosophy & Technology 659, 9.
[341] 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/> accessed 6 January 2021.
[342] 'Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19: Common EU Toolbox for Member States' (n 287).
[343] Monika Kuschewsky, *Data Protection & Privacy: Jurisdictional Comparisons* (Thomson Reuters 2012).
[344] 'What Is SafeEntry?' (*SafeEntry*) <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.

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. **[*Covid Regulation Paper*]**

~

The rights discourse in the pandemic response debate is inevitable, as digital rights advocates and privacy experts identify rushed measures introduced to monitor infections, via digital tracking initiatives and physical monitoring, as merely methods of mass surveillance that constitute digital rights violations.[345] Of course, such a critique depends on the pre-existence of a rights framework and rights protections in the jurisdictions involved and as such, the rights discourse may not have universal purchase. Even in countries with constitutionally enunciated rights, if there is no judicial, executive or administrative appetite for actioning rights claims, or where freedom of speech is politically conditional, the rights discourse may not be as readily adopted by otherwise-compliant communities. **[*Disquiet Paper*]**

5.3 Introducing relevant institutions and processes

The excerpts in this section and the next will emphasise the need for better regulatory strategies and policy interventions to remedy and rectify the inadequacies arising from the language of ethics and rights-based principles. Regulatory strategies must strive towards producing more equitable outcomes for its subjects. Here, Findlay and Remolina propose three particular institutions/processes that seek to promote effective regulatory attainment.

Regulation, whether it be for health and safety assurance, for property rights protection, for market resilience, ensuring universal access and social good, involves a humanist commitment to see the best results for the largest population in this age of uncertainty. Political, hegemonic, economic and philanthropic forces shaping our regulatory responses to the pandemic more than scientific certainty, determine that law will not be applied to the letter of the property rights it ensures if these defy law's own more pervasive normative commitments for justice and fairness. As we argued, the law cannot be blamed if its application produces the opposite results. ***[Vaccine paper]***

~

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), [346] 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. (...)

[345] 'Should I Worry about Mass Surveillance Due to COVID-19?' (n 161).
[346] Findlay (n 197).

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

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. (...)

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*[347] (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.[348]

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 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.

[347] 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 infrastructure will similarly depend on whether the tech and usage dimensions of the response at the time are markedly different from the COVID experience.

[348] 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.

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. ***[Covid Regulation paper]***

5.4 Determining regulatory choice and direction

How might we best understand these proposals? Findlay and Remolina have also sketched out fundamental features that influence a State's regulatory choice and direction. This includes considerations of *why* it is important to regulate, *when* is the appropriate time to regulate or discontinue regulation, *where* should regulation be located, *what* precisely needs to be regulated, and *who* should bear regulatory responsibilities when thinking about the principles of attribution and accountability.

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.[349] 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

[349] Trix Mulder, 'Health Apps, Their Privacy Policies and the GDPR' [2019] European Journal of Law and Technology <https://papers.ssrn.com/abstract=3506805> accessed 6 January 2021; Bobby Fung, 'In This Time of COVID-19, Does Personal Data Privacy Get Thrown out the Window?' *Withers World Wide* (16 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; 'The New EU Regulation on the Protection of Personal Data: What Does It Mean for Patients?' European Patients Forum <https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf>.

of liberties in movement and association.[350] Are the control justifications for employing personal data and restricting liberties valid, or indeed excessive?[351] 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,[352] 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.[353] 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.[354] 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

---

[350] 'Human Rights Dimensions of COVID-19 Response' (n 30); 'Coronavirus Pandemic in the EU–Fundamental Rights Implications' (2020) Bulletin 1 FRA European Union Agency for Fundamental Rights <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.

[351] Suzanne Nossel, 'Don't Let Leaders Use the Coronavirus as an Excuse to Violate Civil Liberties' *Foreign Policy* (13 April 2020) <https://foreignpolicy.com/2020/04/13/governments-coronavirus-pandemic-civil-liberties/> accessed 19 May 2020; Martin J Bull, 'Beating Covid-19: The Problem with National Lockdowns' (*LSE EUROPP (European Politics and Policy)*, 26 March 2020) <https://blogs.lse.ac.uk/europpblog/2020/03/26/beating-covid-19-the-problem-with-national-lockdowns/> accessed 18 May 2020.

[352] 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 and others, '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' [2020] MedRxiv 2020.04.15.20067256; Geofrey Musinguzi and Benedict Oppong Asamoah, 'The Science of Social Distancing and Total Lock Down: Does It Work? Whom Does It Benefit?' (2020) 17 Electronic Journal of General Medicine <https://papers.ssrn.com/abstract=3571947> accessed 6 January 2021.

[353] 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" – Advice Is Political' *The Guardian* (28 April 2020) <http://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.

[354] 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.

location and reach will depend on how much the regulatory recipient wants something to 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.[355] A key strategy in the fight against the virus promoted by North World states[356] 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.[357] 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[358] is the extent to which regulatory recipients identify the need for behavioural change outcomes.[359] 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 particulars.[360] 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.[361] (...)

---

[355] Charles Raab and Benjamin Goold, 'Protecting Information Privacy' (2011) 69 Equality and Human Rights Commission Research Report <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' (2020) Forthcoming The Oxford Handbook of Constitutional Law in Asia <https://papers.ssrn.com/abstract=3548497> accessed 6 January 2021.

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

[357] Mark Findlay, 'Corporate Sociability: Analysing Motivations for Collaborative Regulation' (2014) 46 Institutional Knowledge at Singapore Management University, Research Collection School Of Law 339.

[358] 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.

[359] 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/> 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; Sunstein (n 83).; 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).

[360] 'What Is SafeEntry?' (n 344); 'COVID-19: SafeEntry Digital Check-in System Deployed to More than 16,000 Venues' (n 344).

[361] 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. Bell (n 59); Alex Hern, 'Digital Contact Tracing Will Fail Unless Privacy Is Respected, Experts Warn' *The Guardian* (20 April 2020)

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.[362] 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.[363]

- 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 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

<https://www.theguardian.com/world/2020/apr/20/coronavirus-digital-contact-tracing-will-fail-unless-privacy-is-respected-experts-warn> accessed 28 April 2020.

[362] Michael H Fuchs, 'The US-China Coronavirus Blame Game Is Undermining Diplomacy' *The Guardian* (31 March 2020) <http://www.theguardian.com/commentisfree/2020/mar/31/us-china-coronavirus-diplomacy> accessed 20 May 2020; 'China Emerges as Coronavirus Scapegoat in US Election Campaign' *Al Jazeera* (17 April 2020) <https://www.aljazeera.com/news/2020/4/17/china-emerges-as-coronavirus-scapegoat-in-us-election-campaign> accessed 20 May 2020.

[363] 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. 'Regulatory Quality and COVID-19: Managing the Risks and Supporting the Recovery' (*Organisation for Economic Co-operation and Development*, 29 April 2020) <http://www.oecd.org/coronavirus/policy-responses/regulatory-quality-and-covid-19-managing-the-risks-and-supporting-the-recovery-3f752e60/> accessed 20 May 2020.

provided reporting does not degenerate into misinformation or propaganda for any particular dogma.[364]

- 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.* ***[Covid Regulation paper]***

5.5 Normative foundations

The previous sections have highlighted the critical role of regulation in society. The excerpts below will consider the form that any proposed regulatory strategy or exercise should take. We emphasise three essential normative foundations here. Namely, the need to lessen and avoid discrimination, stakeholders' compliance with ethical and principled design principles, and the importance of promoting citizen inclusion and engagement.

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 [previous sections]. 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 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

[364] Gordon Pennycook and others, 'Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy Nudge Intervention' (2020) 31 Psychological science 770; Jayaseelan R, Brindha D and Kades Waran, 'Social Media Reigned by Information or Misinformation About COVID-19: A Phenomenological Study' (2020) D-20-00130 Social Sciences & Humanities Open <https://papers.ssrn.com/abstract=3596058> accessed 6 January 2021.

- 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. ***[Covid Regulation paper]***

5.6 Adherence to the rule of law in producing effective pandemic responses

The excerpts below seek to draw out the important function of the rule of law (RoL) in producing more effective pandemic response(s). Commitment to the various features of the RoL will help to foster greater public trust, engagement, actionability (in terms of actionable rights and remedies when RoL principles are departed from) and improved governance. In combination with ethics, a State's adherence to RoL principles will enhance its legitimacy and influence over citizens' overall willingness to comply with the introduced measures.

In their report 'The Rule of Law in Times of Health Crises'[365] Julinda Beqiraj, Jean-Pierre Gauci and Nyasha Weinberg identified certain conditions under which rule of law adherence can contribute to an effective pandemic response. These include:

- Transparency
- Clarity
- Participation, engagement and representation
- International cooperation
- Equality and equity
- Accountability and anti-corruption

In the context of pandemic control strategies and public reaction, the first three of these are particularly directed toward better ensuring public trust and citizen engagement. The remainder say something about governance responsibilities in the use of personal data. A quick comparison of the language used to describe these conditions and the central ethical principles espoused in AI ethics frames[366] suggests aspirational commonality between rule of law and ethical discourse. Both ethics and rule of law compliance are meant to create an operational consciousness among designers and users of AI-technologies such as have been advocated and employed in COVID-19 control.[367] In addition, the mass personal data sharing potentials emerging out of these surveillance technologies have generated community disquiet[368] that requires the reassurance of some recognition of individual rights and liberties. (...)

Rule of law discourse shares many of the principles espoused in AI ethics discourse. What sets rule of law apart is its essential connection with;

- A constitutional 'backbone' that gives definitive comparative measure against which self-regulation can be empirically reflected, and
- An inextricable connection to fair and just processes for effecting and actioning rights and remedies which normative principles originally determine but do not enforce.

At present, the Centre for AI and Data Governance is researching how certain structural inequalities in society mean that particular groups and communities are more vulnerable to pandemic heath risks, and that choices concerning control strategies employed towards these vulnerabilities can exacerbate discrimination. Rule of law, with its commitment to equality, impartiality and fairness goes to the heart of this concern. Not only can rule of law ascription identify pre-existing inequality, and subsequent discrimination but it also is able to direct remedial processes for citizen inclusion (constitutional engagement) and rights activation (legal remedy provision). (...)

---

[365] Julinda Beqiraj, Jean-Pierre Gauci and Nyasha Weinberg, 'The Rule of Law in Times of Health Crises' [2020] Bingham Centre for the Rule of Law <https://binghamcentre.biicl.org/publications/the-rule-of-law-in-times-of-health-crises> accessed 11 July 2020; Julinda Beqiraj, Lucy Moxham and Anthony Wenton, 'Unity and Diversity in National Understandings of the Rule of Law in the EU' [2020] Bingham Centre for the Rule of Law <https://binghamcentre.biicl.org/publications/unity-and-diversity-in-national-understandings-of-the-rule-of-law-in-the-eu-reconnect-deliverable-71> accessed 15 July 2020.

[366] Eduardo Magrani, 'New Perspectives on Ethics and the Laws of Artificial Intelligence' (2019) 8 Internet Policy Review <https://policyreview.info/articles/analysis/new-perspectives-ethics-and-laws-artificial-intelligence> accessed 20 July 2020.

[367] Soumya Banerjee, 'A Framework for Designing Compassionate and Ethical Artificial Intelligence and Artificial Consciousness' (2018) 18 Interdisciplinary Description of Complex Systems 85.

[368] 'Singaporean Attitudes to Personal COVID Data Differ to Overseas Counterparts' (n 68).

The first constituent of my contention that rule of law requires action for it to adequately address the legitimacy crisis facing the normative/principled frames for regulation of AI, is inclusivity. A trawl through rule of law discourse recognises the importance citizen inclusion in achieving equality, accountability, transparency and certainty. If procedural justice is to be asserted in policymaking, particularly when it is tested in the exigencies of a health pandemic then the reassurance from a provident and paternal state can only go so far without the bolstering of representative citizen engagement. (...)

In keeping with this empowerment theme, the second constituent is the actionability/enforcement of rights and remedies. In their discussion of the relationship between rule of law principles and responses to public health emergencies, Beqiraj, Gauci and Weinberg[369] identify the necessity for non-derogable rights to be protected absolutely and other rights to connect with effective remedies for challenging the legitimacy of derogation measures. It is at the level of enforcement that the rule of law in action parts ways with normative/principled regulatory frames which rest on voluntary compliance and perhaps a touch of reputational shaming. ***[ROL paper]***

5.7 Societal inclusion and democratic participation

As highlighted in the above section, adherence to principles of the rule of law will enhance societal inclusion and democratic participation. The rule of law as a regulatory regime also supports the delivery of a mechanism for actionability when individual rights are put at risk or are disregarded. This emphasis on inclusion, participation, and actionability is critical in our remedying of the above-identified challenges and our consideration of how State legitimacy and trust outcomes can be improved. At the end of the section, Wee and Findlay narrow in on Taiwan's collaborative approach with its citizen hackers and showcase how citizen inclusion can be achieved in practice.

[A] reading of the many expressions of community concern about the possible negative impact of pandemic surveillance technologies on freedom of association and movement, and challenges to individual integrity, suggests they can be reduced to these fundamentals: inclusion and actionability. In democratic nation states where accountability and representation are essential conditions for governance legitimacy, distrust surrounding exceptional surveillance regimes will not only impact on the effectiveness of such technologies to achieve their anticipated prevention and control purposes[370], but may undermine a wider attitude of amenability and obedience to intrusive pandemic responses or those which depend on simple and recurrent attitudes of acceptance and cooperation. (...)

[Addressing the challenges to rule of law posed by pandemic responses] require active participation from the citizenry in policy formulation and roll-out if the governance expectations of justice, fairness, equality, explainability and answerability are to mean much more than vague ethical endowment. (...)

Without the essence of democratic participation, in the form of citizen integration in emergency policymaking, and actionability if rights and liberties are compromised (both features of 'thick

[369] Beqiraj, Gauci and Weinberg (n 365).
[370] Mark Lawrence Schrad, 'The Secret to Coronavirus Success Is Trust' (*Foreign Policy*, 15 April 2020) <https://foreignpolicy.com/2020/04/15/secret-success-coronavirus-trust-public-policy/> accessed 20 July 2020.

rule of law)[371] then the regulatory legitimacy crisis facing principled regulatory regimes remains. ***[ROL paper]***

~

Grass roots Transparency and Accountability[372]

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[373] justifying restrictions on certain rights,[374] then causal relations between threat, 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."[375] 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

---

[371] Brian Z Tamanaha, *On the Rule of Law: History, Politics, Theory* (Cambridge University Press 2012).
[372] Header from original paper.
[373] 'Coronavirus Disease (COVID-19) Pandemic' (*World Health Organisation*) <https://www.who.int/emergencies/diseases/novel-coronavirus-2019> accessed 6 April 2020.
[374] For instance, such as those that result from the imposition of quarantine or isolation limiting freedom of movement. See Andrea Salcedo, Sanam Yar and Gina Cherelus, "Coronavirus Travel Restrictions, Across the Globe", *The New York Times* (15 April 2020) <https://www.nytimes.com/article/coronavirus-travel-restrictions.html> (accessed 7 April 2020)
[375] See 'International Covenant on Economic, Social and Cultural Rights' (n 283). 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.
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 'CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)' (n 283).

through recurrent and structured community consultations and conversations.[376] ***[Covid Regulation paper]***

~

However, it would be incorrect to suggest that distrust is universal or that it has completely eroded public confidence in control technologies. Professor Yuval Noah Harari proposed that instead of building a permanent surveillance regime as remedy for pandemic threats ongoing, there is still time to "rebuild people's trust in science, in public authorities and in the media".[377] This alternative approach to omniscient technology and state paternalism may be achieved by empowering citizens via *inclusion in the development and maintenance of AI-assisted control technology,* providing greater opportunities to hold the policymakers and surveillance proponents accountable for decisions that endanger rights and liberties. By ensuring greater transparency of data, control information and policy details through techniques such as information loops, citizens will be able to monitor their government's data management and judge for themselves whether the data managers and repositories are adhering to ethical principles and respecting citizens' interests. With greater civilian inclusion, users can make informed personal choices about what technology they will tolerate and why, and may as a consequence, be more willing to participate in contact tracing activities.[378] (...)

Taiwan's collaborative approach with citizen hackers[379]

In Taiwan, Digital Minister Audrey Tang has won praise for utilizing control tech to facilitate effective COVID-19 control responses. As of the time of writing, Taiwan reported a total of 489 cases[380] out of its nearly 24 million citizens.[381] The low infection rates are attributed to civic co-operation, owing to the fact that digital disinformation has largely been addressed by an existing architecture of a "[large] digital literacy of civic engagement" implemented prior to the pandemic.[382]

Previously, the Taiwanese administration acknowledged civic disengagement and sought to remedy that by approaching a group of civic-minded hackers and coders, g0v,[383] who are devoted to improving government transparency through the creation of open-source technologies.[384] Collaboration with the government resulted in the setting up of platforms, e.g. vTaiwan[385] and Pol.is,[386] which allow for public representatives and private organizations to

---

[376] 'Mobile Applications to Support Contact Tracing in the EU's Fight against COVID-19: Common EU Toolbox for Member States' (n 287).
[377] Yuval Noah Harari, 'Yuval Noah Harari: The World after Coronavirus | Free to Read' (20 March 2020) <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75> accessed 27 July 2020.
[378] Harari (n 377).
[379] Header from original paper.
[380] 'Coronavirus (COVID-19)' (*Google News*) <https://news.google.com/covid19/map?hl=en-SG&gl=SG&ceid=SG:en> accessed 3 September 2020.
[381] Christina Farr Gao, 'How Taiwan Beat the Coronavirus' (*CNBC*, 15 July 2020) <https://www.cnbc.com/2020/07/15/how-taiwan-beat-the-coronavirus.html> accessed 3 September 2020.
[382] 'How Taiwan's Unlikely Digital Minister Hacked the Pandemic' *Wired* <https://www.wired.com/story/how-taiwans-unlikely-digital-minister-hacked-the-pandemic/> accessed 31 August 2020.
[383] 'G0v.Asia' <http://g0v.asia/> accessed 3 September 2020.
[384] Audrey Tang, 'Opinion | A Strong Democracy Is a Digital Democracy' *The New York Times* (15 October 2019) <https://www.nytimes.com/2019/10/15/opinion/taiwan-digital-democracy.html> accessed 31 August 2020.
[385] 'VTaiwan.Tw — 數位經濟法規線上諮詢' <https://vtaiwan.tw/> accessed 3 September 2020.
[386] 'Polis' <https://pol.is/home> accessed 3 September 2020.

debate policy solutions, including those in the digital economy, and property tax issues, etc. These platforms provide for greater facilitation (and generation) of ideas among participating parties, while also allowing the government quicker and more direct insights into what the public requires.[387] Minister Tang herself advocates for a "radical transparency" approach to her work, where she opens her office up for 40 minutes at designated times for individuals or organizations to approach her, whether to interview her or lobby for ideas. Radical transparency encourages the engagement of "thoughtful disagreement" and the productive, honest exchange of controversial ideas within organisations and democracies in the hope of fostering an environment of openness among all parties.[388] One condition that Minister Tang has for her meetings is that each of the sessions be uploaded online via textual transcripts (where participants are allowed to edit texts and anonymise themselves prior to the publication),[389] to recognise and amplify the best voices in society.[390]

In the context of the pandemic, a citizen-developed tool was devised to track the availability of medical masks in nearby pharmacies using a distributed ledger technology.[391] Engineer and civic hacker, Howard Wu, created a website using Google Maps aimed to provide information on mask availability based on information voluntarily given by the public.[392] This enabled for public contribution of real-time stock taking, where those with masks would show up as green on the app, while out-of-stock stores would turn red.[393] When Minister Tang heard of Wu's mask map, she met with the Premier to propose new ways to fine-tune the mask-rationing system. Then, Minister Tang posted the news of the approved tracking system to a Slack channel, where Taiwan's civic tech hackers were invited to use the data as they wished.[394] As the map gained greater traction within the nation, more hacking teams soon added features including, most notably, a voice-control option for the visually impaired.[395] Tang pointed out that this was the first time in which hackers felt like they were the designers, and owners, of a civil engineering project. ***[Disquiet paper]***

5.8 Sectorial specific regulation

The following section embarks on a sector-specific examination into the regulations of financial markets during the pandemic. It introduces and reflects on an appropriate legal model for financial markets to illustrate how law and finance may be understood as positive correlations, thereby promoting market sustainability and resilience. This is followed by an examination of the challenges that have arisen from the digital

[387] Tang (n 384).
[388] Francesca Gino, 'Radical Transparency Can Reduce Bias — but Only If It's Done Right' [2017] *Harvard Business Review* <https://hbr.org/2017/10/radical-transparency-can-reduce-bias-but-only-if-its-done-right> accessed 11 September 2020.
[389] 'Audrey Tang - We Have to Keep Defining What Is the Inter in Internet' (*Framer Framed*) <https://framerframed.nl/dossier/audrey-tang-we-have-to-keep-defining-what-is-the-inter-in-internet/> accessed 3 September 2020.
[390] 'Three Ways Taiwan Is Adapting to the New Normal' (*GovInsider*, 17 June 2020) <https://govinsider.asia/innovation/could-government-change-permanently-after-covid-19-audrey-tang-taiwan/> accessed 31 August 2020.
[391] 'Three Ways Taiwan Is Adapting to the New Normal' (n 390).
[392] Michal Chabinski, 'Getting Civic About Technology' (4 August 2020) <https://www.echo-wall.eu/currents-context/getting-civic-about-technology>.
[393] 'How Taiwan's Unlikely Digital Minister Hacked the Pandemic' (n 382).
[394] 'How Taiwan's Unlikely Digital Minister Hacked the Pandemic' (n 382).
[395] Shiroma Silva, 'How Map Hacks and Buttocks Helped Fight Covid-19' *BBC News* (7 June 2020) <https://www.bbc.com/news/technology-52883838> accessed 17 August 2020.

transformation of the banking sector and some regulatory recommendations to promote an inclusive and sustainable recovery in the post-pandemic financial industry.

Regtech - Anti-money laundering, know your customer and tracing fraudulent transactions[396]

In recent years, especially after the 2008-2009 global financial crisis, financial institutions have been exploring ways of reducing operational costs and being more efficient. Therefore, the digital transformation processes of the fintech age have positively impacted compliance processes. In particular combating money laundering is an enormous task, and it comes with substantial costs and risks, including but not limited to regulatory, reputational and financial risks. Hence, industry participants and regulators welcome new ways to sharpen surveillance on an ongoing basis for the purposes of effectively satisfying government financial transaction reporting requirements.

Banks have taken steps to work with different players in the *regtech*[397] ecosystem to combat money laundering using Machine Learning ("ML") and AI. Traditional ways of surveillance are less successful, resulting in large numbers of false positives (95% in some banks).[398] Additionally, since the global financial crisis, financial institutions are looking into ways of making their compliance much more efficient, making regtech very popular in recent years.[399]

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

Financial institutions also use regtech to analyse millions of documents and check details against 'blacklists' for the know-your-customer ("KYC") checks before the on-boarding account opening process begins. Particularly banks are increasingly using ML to rate the likelihood of a customer posing a financial crime risk, and as customers transfer money or make payments, firms use machine learning to identify suspicious activities and flag potential cases, so human analysts can focus on these specifically.[400]

---

[396] Header from original paper.

[397] RegTech can be defined as the use of technological solutions to facilitate compliance with and monitoring of regulatory requirements. In recent legal doctrine, RegTech is almost unequivocally hailed as holding the promise of substantial gains in terms of increased efficiency and reduced risk of human errors and resulting administrative fines. See Veerle Colaert, 'RegTech as a Response to Regulatory Expansion in the Financial Sector' <https://papers.ssrn.com/abstract=2677116> accessed 5 January 2021; Douglas W Arner, Janos Nathan Barberis and Ross P Buckley, 'FinTech, RegTech and the Reconceptualization of Financial Regulation' <https://papers.ssrn.com/abstract=2847806> accessed 5 January 2021.

[398] Joshua Fruth, 'Anti-Money Laundering Controls Failing to Detect Terrorists, Cartels, and Sanctioned States' *Reuters* (15 March 2018) <https://www.reuters.com/article/bc-finreg-laundering-detecting-idUSKCN1GP2NV> accessed 2 July 2021.

[399] Arner, Barberis and Buckley (n 397).

[400] Carsten Jung and others, *Machine Learning in UK Financial Services* (Bank of England and Financial Conduct Authority 2019) <https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf> accessed 27 April 2020.

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

- *Human in the loop*: For the KYC tools, human analysts continue to play a decisive role in the process.[401] Once alerts are raised, analysts can narrow their focus to these more relevant sources. At the more advanced end, tools have the capacity to output a 'next step' for the analyst, who may agree or disagree with the decision. Firms say this helps improve the performance of the model because the system will adapt and refine its options on further use depending on the human decision.

- *Fairness and explainability*: Adherence to data protection policies, fair use of personal data and the legal right to explanation are important considerations in deciding on the scope of data used to train and operate the AI as well as outputs and information that can be shared by the AI. Financial institutions must be prepared to explain the details of the model, how it works, and to explain the decisions that the approach makes to avoid compliance breaches. Employing an army of data scientists is not enough – though likely highly skilled in technology, having the layer of financial crime domain expertise on top of that is essential in an intricate and highly-regulated field.[402]

  For transaction monitoring, the main complexity issues arise from the management of IT infrastructure and the oversight of data pathways and validation, according to the Financial Conduct Authority ("FCA").[403] Tools of a high technical complexity often combine a range of Machine Learning methods to draw insights on customers. The input data is of all structures,[404] and the explainability of the learning process is of great interest to firms deploying such tools[405] given that banks, in most jurisdictions, justify why a particular customer or transaction is flagged. Therefore, their interest to break down the unsupervised learning procedure of neural networks of a machine learning tool for transaction monitoring.

- *Transparency and auditability*: The ability to demonstrate and audit compliance is a cornerstone of the current anti-money laundering ("AML") framework — so the transparency of AI and its underlying algorithms is important. AI and machine learning are broad fields with varying levels of complexity and transparency. At the more complex end of the spectrum, neural networks and deep learning may prove more difficult areas in which to build trust, when compared with more existing processes. At present, very few of the current AML solutions being trialed in banks have advanced beyond regression, decision trees and clustering due to these challenges.

- *Data quality and training*: Data quality is a major challenge for many financial institutions and often impacts the effectiveness and efficiency of AML controls.

[401] Jung and others (n 400).
[402] Chad Hetherington, '"Explainable AI": The Next Frontier in Financial Crime Fighting | NICE Actimize' (*NICE Actimize*, 25 February 2019) <https://www.niceactimize.com/blog/explainable-ai-the-next-frontier-in-financial-crime-fighting-595/> accessed 27 April 2020.
[403] Particularly in UK. Jung and others (n 400).
[404] In computer science, a data structure is a data organization, management, and storage format that enables efficient access and modification. More precisely, a data structure is a collection of data values, the relationships among them, and the functions or operations that can be applied to the data. There are generally four forms of data structures: linear, tree, hash, graphs. See Mark McDonnell, 'Data Types and Data Structures' (*Integralist*, 30 January 2019) <https://www.integralist.co.uk/posts/data-types-and-data-structures/> accessed 13 April 2020.)
[405] Jung and others (n 400).

Projects need to assess data quality and its appropriateness for use by AI as part of the design and development phase, and also implement data management controls to monitor the ongoing data quality during operation and how model are trained. Recent cases in the financial industry have gone wrong already (mostly in credit scoring, not in AML).[406]

Suptech - Misconduct and Market Surveillance by Financial Regulators[407]

Some financial regulators are using AI for market surveillance and fraud detection, which is also known as *suptech*. [408] For instance, the Australian Securities and Investments Commission ("ASIC") has been exploring the quality of results and potential use of Natural Language Processing ("NLP") technology to identify and extract entities of interest from evidentiary documents.[409] ASIC is using NLP and other technology to visualise and explore the extracted entities and their relationships. In order to fight criminal activities carried out through the banking system (such as money laundering).

The FCA performs network analysis on orders and executions data to construct webs of market participants and identify collusive behaviour indicating insider trading, while the Netherlands Bank ("DNB") employs a similar technique to link individuals sending funds to the same counterparties in high-risk jurisdictions along various routes.[410]

Market regulators can also use these techniques for disclosure and risk assessment. The US Securities and Exchange Commission ("SEC") staff leverages "big data" to develop text analytics and machine learning algorithms to detect possible fraud and misconduct. For investment advisers, the SEC staff compiles structured and unstructured data. Unsupervised learning algorithms are used to identify unique or outlier reporting behaviours – including both topic modelling and tonality analysis. The output from this first stage is then combined with past examination outcomes and fed into a second-stage, machine learning algorithm to predict the presence of idiosyncratic risks at each investment advisor.[411]

Despite the benefits that these early adopters are exploring by using technology in their surveillance processes, they also recognise challenges and risks of this type of surveillance. First, use of suptech without taking the necessary measures to address technical, data quality, legal, operational, reputational, resource, internal support and practical issues may expose supervisors to undue risks.[412] Moreover, although suptech can help identify potential issues and problems, human intervention is necessary to pursue further investigations and decide on a

[406] Patrick Craig, 'How to Trust the Machine: Using AI to Combat Money Laundering' (*EY*, 3 September 2019) <https://www.ey.com/en_in/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering> accessed 27 April 2020.
[407] Header from original paper.
[408] Suptech refers to the application of big data or artificial intelligence (AI) to tools used by financial authorities. See Simone di Castri and others, 'The Suptech Generations' (2019) FSI Insights on policy implementation Bank for International Settlements <https://www.bis.org/fsi/publ/insights19.pdf>.
[409] Jamie Smyth, 'Australian Regulators Cautiously Embrace AI to Boost Compliance' *Financial Times* (8 April 2019) <https://www.ft.com/content/33eb5934-4519-11e9-b168-96a37d002cd3> accessed 27 April 2020.
[410] Suptech refers to the application of big data or artificial intelligence (AI) to tools used by financial authorities. See Castri and others (n 408).
[411] 'Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications.' [2017] Financial Stability Board 45.
[412] Dirk Broeders and Jermy Prenio, 'Innovative Technology in Financial Supervision (Suptech): The Experience of Early Users' 9 FSI Insights on policy implementation 2018.

suitable course of action.[413] Second, according to the Financial Stability Institute, supervisory agencies also need to be cautious of a growing data-knowledge gap. On one hand, data availability, data quality and data storage facilities are improving rapidly, as are techniques for combining different data sources. On the other hand, data analytics may not be advancing at the same pace. It takes time to learn, develop and implement new technologies in supervision work. Agencies could make an assessment of data availability and to what extent data is being fully used in supervision work.[414] ***[Ethics paper]***

~

Despite the neoliberal logic to the contrary (where financial markets are deemed only for maximising investor/shareholder profit) financial market regulation should prioritise market sustainability as part of pandemic control policy. (...) [It is necessary] to reflect on a legal model for financial markets, their regulation, and its limitations so that law and finance may be understood as positively relational when considering market sustainability. (...)

The resonance with contemporary concerns about fake news (surrounding such issues as effective COVID-19 drugs) and its impact on stock trading is uncanny, as are the calls for legal regulatory intervention.

If the nature and riskiness of information on which market decisions are made is a factor in the disconnect so far identified, and therefore it is argued a focus for regulatory attention, can law play a part in achieving objectives for market sustainability and resilience? In answering this question, it is useful to explore a legal theory of finance.

A legal model for the Financial Market[415]

The neoliberal Washington Consensus desiderata is for a deregulated financial market, without which wealth maximisation cannot be realised. Joh Braithwaite in his compelling analysis of mega multi-national capitalism dispelled this fiction, by establishing that it was an explosion in regulation in all its forms which enabled the massive market surges of recent times.[416] Accepting for the sake of argument that regulation is not the antithesis of a healthy financial market, the next question is, what model might best ensure market profitability and sustainability, rather than fiddling with some crude regulatory pressure valves. To make an informed determination it is necessary first to settle on a theory of the market which anticipates and encapsulates legal regulation.

In her paper 'A Legal Theory of Finance' Katharina Pistor[417] argues that financial markets are legally constructed and as such occupy a hybrid (regulatory) space between the state and the market, the public and the private. Now this makes sense because the institutional core of financial markets which is the corporation, is a legal fiction, without form or substance but for law. Even so, as Pistor observes, financial markets exhibit dynamics that frequently put them at odds with commitments in both public and private law. She asserts that the law/finance

[413] Broeders and Prenio (n 412).
[414] Broeders and Prenio (n 412).
[415] Header from original paper.
[416] John Braithwaite, *Regulatory Capitalism: How It Works, Ideas for Making It Work Better* (Edward Elgar 2008).
[417] Katharina Pistor, 'A Legal Theory of Finance' (2013) 41 Journal of Comparative Economics 315.

tension tends to be resolved in times of crisis by suspending the full enforcement of the law where market survival is at stake. Once this occurs, she reverts to a power analysis.

Useful as is her endeavour to establish a legal model for the financial market, and necessary as this would be if law is to play a role in effective market regulation to return the financial market to the social, there are two obvious flaws in Pistor's compromise. First, a power analysis of any market is not simply the product of law's recession. Markets are structured around power dynamics inherently. The basic concept of the exchange market is that someone has surplus that they wish to commodify, and this is a power relationship between buyer and seller, depending on the externalities governing supply and demand. Therefore, a legal model for the financial market necessarily operates within and beyond prevailing market forces and dispersals. The second misconception, perhaps based on the earlier mentioned myth that market profitability and regulation are antithetical, enforcing law, and thereby creating certainty, which is essential for market predictability, will not lead to market meltdown, no matter how powerful market players argue to the contrary.

The legal theory of the financial market is based on two premises, fundamental uncertainty and liquidity volatility, reinforced by law:

> The two go together: If the future were known we could take precaution to deal with future liquidity scarcity; if liquidity were always available on demand, i.e. a free good, we could refinance commitments as needed when the future arrives…LTF's critical contribution is to emphasize that the legal structure of finance is of first order importance for explaining and predicting the behaviour of market participants as well as market-wide outcomes.

Such an elaboration well represents the dynamics of financial markets in the current pandemic context when uncertainty and liquidity volatility are devoid of even much private law constraint. Hence, while wealth creation may be short term, peaks and troughs in market flow are inevitable in the short to medium terms. The solution to volatility may not rest in refining predictability. In fact, certain unpredictability and volatility situations may lead to short term profit taking. However, if the objective of regulation is to preserve financial stability, this may differ from predictability. Financial stability is achieved in large measure by risk-based regulation, which is supposed to incentivize players in a financial market to being capable to absorb losses depending on the risks they take – this is applicable particularly to banks. That is why designated financial institutions with fiduciary obligations to a broad client base cannot engage in certain speculative activities. They have to be capitalised depending on the risks they take, they have to be stress tested on the basis of hypothetical stressed macroeconomic scenarios, etc. Additionally, in the world of capital markets – not so much in the banking sector, even though both worlds collide – it may be more important for regulators to address asymmetries of information, rather than how predictable markets are. Even so if unpredictability in markets is to be tolerated so that some investors enjoy profit through associated speculation and risk taking, that does not deny regulators the opportunity to employ law to achieve a more certain understanding of the consequences of risk and speculation. Greater certainty in appreciating the consequences of market choice will enhance sustainability while not requiring that every risk be predictable. In some styles of risk analysis, while a particular dangerous consequence is not possible to predict in terms of temporal and spatial accuracy, if the negative outcome is certain at some time or place then regulators have the challenge to avoid that eventuality.

Noting what she refers to as contemporary facts about finance Pistor suggests financial assets are legally constructed, law contributes to financial instability, finance is inherently hierarchical, and the binding nature of legal and contractual commitments tends to be inversely proportional to finance's hierarchy (that is law has a more productive regulatory influence on the periphery of a financial system).

Interestingly, by focusing on what the theory sees as law's elasticity, the regulatory vision is one where law is not performing command and control functions but is more likely to assume negotiable private law arrangements which become more flexible as the market hierarchy is scaled. Again, this presents a limitation in applying law as a more stringent enforcement mechanisms, in market settings that have thrived through risk-taking an irresponsibility.

Moving on from the theory's interest in what it refers to as the law/finance paradox (which again can be criticised as a duality based on contestable neoliberal assumptions regarding market dynamics – such as profit over sustainability) attention is drawn to 'power as the differential relation to law'. In explaining this connection Pistor argues:

> Power is exercised throughout the financial system. It is exercised by those who have the resources to extend support to others without being legally obliged to do so. Those who have access to unlimited resources have the most power: Sovereigns with control over their own currency and debt. Their access to unlimited resources derives from their power to issue the legal tender, to use their means of coercion to levy taxes on their subjects and to coordinate political and economic resources to make credible their commitments (Kapadia 2013). The absence of any of these three conditions can undermine the credibility of a sovereign as effective lender of last resort. By the same token it positions the sovereign towards the periphery of the global hierarchy of finance.

As a consequence of this reasoning positioning in the financial hierarchy is a matter of power and not simply of law. So, where does this locate law in its regulatory role over finance?

> Taken together, the elements of LTF suggest that law is central to finance in at least three respects: Law lends authority to the means of payment; it spurs regulatory pluralism by delegating rulemaking to different stakeholders and in doing so helps draw boundaries between different markets; and it vindicates financial instruments and other financial contracts. State authorized and backed money serves as the backbone of modern financial systems. It is the common reference price for all other assets; it is also the asset of last resort when others no longer find takers. Further, law sets the stage for legal pluralism by determining which actors, activities and instruments to regulate and which to leave to private regulation. The greater the tolerance for competing regulatory regimes, the greater the probability that competition will increasingly take the form of regulatory arbitrage, i.e. the gaming of the very system that makes and shapes finance. Last but not least, law recognizes contracts and defines the contours of their enforceability. This enhances their credibility, but to the extent that financial instruments are designed to weaken regulatory costs it effectively sanctions regulatory arbitrage and the erosion of formal law. (...)

[...] Employing a modified legal theory of finance and reflecting on Polanyi's double movement, regulators are well advised to direct an initial regulatory focus on developing more uniform information 'commodities' that make sense of the financial market **and** the economy

in decline. If this is achieved, then the risks associated with self-regulating markets could be more commonly surveyed.

There are several assumptions on which this paper's regulatory invocations rely

1. That in times of economic crisis such as this pandemic, and situations where the financial market and the economy significantly diverge, the objective for regulating financial markets (particularly self-regulating markets) is market sustainability and resilience.
2. A disconnect between financial markets and the economy in terms of risk evaluation and market activity can endanger market sustainability and resilience if a counter movement in the economy and the social is not managed effectively. The consequences of market bubbles need to be avoided proactively.
3. The law can be employed to create greater levels certainty in the market in order to minimise or avoid catastrophic risk outcomes.
4. Law's elasticity (rather than its mandatory enforcement capacity) makes it compatible with market fluidity, even in times of crisis.
5. In crisis regulation, the law is not necessarily employed to improve risk predictability for investor benefit or otherwise.
6. Nominating sustainability and resilience as regulatory priorities for market regulation may mean a reduction in short-term investor profit, in times of crisis and post crisis recovery.
7. A practical target for legal regulation is the reduction in information asymmetries between the financial market and the economy.
8. Targeting information asymmetries should not be restricted to instances of conscious market manipulation but regulators should concentrate on enhancing information accuracy to facilitate market choices based on a more certain understanding of consequences for sustainability and resilience.

In the pandemic, investors like all responsible citizens share an obligation to keep the community safe. This obligation extends to informed market decision-making which goes beyond self-interest. More than being a 'call to arms' for regulators who should be concerned about the possible negative consequences of the disconnect between financial markets and the economy, the paper's argument has endeavoured to establish that the disconnect is evidence of extreme social dis-embedding and as such represents a danger to political and general economic recovery policy.

Consistent with directing regulatory energy to information essential for market dynamics and decision-making consequences, regulation to shield the financial market, the economy and their sustainability will need to responsibilise the protection of investor profit, recognising the two objectives are not mutually exclusive. The inherent problem with the prevailing financial market wisdom that the *riskier product* the greater the profit and therefore 'let the buyer beware' is the reality in times of crisis that such approaches jeopardise much more than individual investor wealth creation. Polanyi would agree, the more fictitious the commodity the more the risk its transaction represents, but in there lies a fundamental question of how law should structure a sustainable market which thrives on internally generated information and speculative profit prediction.

With pandemic control having wider economic ramifications for the safety of society, I am not arguing for law as an agent of market certainty/predictability and acting as risk management

variable primarily protecting investor profit. This analysis is more interested in law addressing fundamental information asymmetries at the heart of the disconnect so that certain risk taking, with adequate information is no longer an indicator of speculative and sometimes irresponsible market choice. Despite the neoliberal logic to the contrary (where financial markets are deemed only for maximising investor/shareholder profit) regulation should prioritise market sustainability as part of pandemic control policy. The clear regulatory objective when markets are radically dis-embedding, should be not only making risk more predictable but instead making the foundations and consequences of risk more certain and as such to introduce measures of responsible market behaviour.[418] ***[Polanyi paper]***

~

[Despite the potential benefits of the digital transformation, the future of data-driven finance in a post-pandemic world looks challenging and encompasses many risks for consumers and the stability of the financial sector and for financial inclusion. Hence, an adequate balance of different regulatory objectives will be crucial for a sustainable and inclusive recovery in a post-pandemic financial industry.]

An inclusive recovery through data analytics and artificial intelligence[419]

Policymakers must promote an inclusive recovery, one that benefits all segments of society. Governments around the world have deployed extraordinary policy measures to save lives and protect livelihoods. These include extra efforts to protect the poor, with many countries stepping up food aid and targeted cash transfers. Globally, fiscal actions so far amount to about $10 trillion.[420] (...)

The data-driven finance, if adequately deployed, can contribute to this inclusive recovery. A key priority must be to broaden the access of low-income households and small businesses to financial products. (...)

Enhancing credit risk management through data initiatives to promote an inclusive recovery will be crucial in the post-pandemic. In the post-pandemic, the lending ecosystem will have to work towards 4 goals that might help enhance credit risk management effectively.

First, building a dynamic credit decisioning framework and credit scores that incorporate the potential impact of the pandemic is key. The traditional credit scoring may need to be remodelled to take into account the potential impacts of pandemic and to include additional information about those potential lenders that are not yet included in traditional databases, for example by using alternative data. This approach will help artificial intelligence and machine learning to score more adequately the credit risks of borrowers.

---

[418] The discussion of the importance of introducing measures of responsible market behaviour is a timely debate because of the clash between hedge funds (acting as shadow banks) and some regulators. Regulators are calling for tougher oversight since the global financial crisis, but little has been done in that space. See Rich Miller and Jesse Hamilton, 'Fed Headed for a Clash With Hedge Funds, Other Shadow Banks' *Bloomberg* (3 August 2020) <https://www.bloomberg.com/news/articles/2020-08-03/fed-is-headed-for-a-clash-with-hedge-funds-other-shadow-banks?utm_source=url_link>.

[419] Header from original paper.

[420] Kristalina Georgieva, 'The Global Economic Reset—Promoting a More Inclusive Recovery' (*International Monetary Fund Blog*, 11 June 2020) <https://blogs.imf.org/2020/06/11/the-global-economic-reset-promoting-a-more-inclusive-recovery/> accessed 8 January 2021.

Second, banks and digital lenders will have to deal with the fact that the crisis will dramatically increase non-performing loans, although with temporary relief from strict regulations and with massive liquidity help from central banks. Restructuring in the sector will accelerate. An open question is whether surviving incumbents will move ahead or if powerful new players - such as Big Tech - will enter the sector with force, transforming the incumbents.

Third, a targeted approach in redesigning loan terms or products for existing borrowers. The potential impact of the pandemic would not only be different among sectors but even among borrowers within sectors. In redesigning the terms for existing borrowers, the intervention can be targeted to individual accounts by considering borrower-specific characteristics and circumstances such as age, employment status, industry employed in, credit history, COVID-19 cases in their province/city, among others. A similar approach can be done to corporate clients. For example, a borrower owning a restaurant is different to a borrower that is a bank. Even borrowers in the same sector might differ a lot considering factors such as the location of the business. Machine learning models used for clustering debtors may enable this targeted approach in redesigning terms.

However, is important to address the potential challenges that this theoretical benefits of enhancing credit risk management effectively through data analytics and artificial intelligence represent. The use of Artificial Intelligence and Machine Learning for credit scoring and credit risk management comes with critical challenges associated with fairness and discrimination in credit lending practices that regulators need to rapidly address. (...)

Up to date, we are starting to witness the first cases of discrimination and unfair lending practices that can even not only affect borrowers directly, but can also create negative externality and even compromise the stability of the financial system. For instance, the Australian Securities and Investments Commission decided in July 2020 that it will not appeal the dismissal of its case against a fintech called Westpac. Instead, it will review its existing guidance on responsible lending and recommend legislative reforms. Westpac was charged in 2017 for having improperly assessed whether loans were suitable for customers (between 2011 and 2015). The Federal Court ruled that Westpac's use of the Household Expenditure Measure benchmark was compliant with responsible lending laws, despite it representing a low-end estimate of the spending habits of Australian families.[421] This could be a good opportunity for Australian regulators to review how they should target fair lending practices and the use of data and Artificial Intelligence in lending. It is a much needed policy discussion in all jurisdiction though.

Online lenders and digital payments vulnerability[422]

On the one hand, online small-business lenders have become the main source of credit for many companies, especially for SMEs and highly vulnerable small businesses. However, currently online lenders are paralyzed because they cannot access funding on which their business

[421] See '20-166MR ASIC Will Not Appeal Federal Court Decision on Westpac's "Responsible Lending" Obligations' (*Australian Securities & Investments Commission*, 22 July 2020) <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-166mr-asic-will-not-appeal-federal-court-decision-on-westpac-s-responsible-lending-obligations/> accessed 8 January 2021.
[422] Header from original paper.

depends. As a result, they are scaling back – just when their services are most needed.[423] An online lender is no different than a finance company that needs to borrow in the capital markets and lend that money to customers. When funding in the capital markets is unavailable or very expensive, a finance company quickly hits the wall and will not be able to provide new credit to its customers.[424] The marketplace lending business model of many online lenders only exacerbates the crisis funding problem. That means online small-business lenders need governments' help, in the short and medium-term, rescue their customers and then to play a meaningful role in any small business credit and economic recovery.[425] This is something to take into account in the post-pandemic world: recognize the different approaches that digital lending – specially provided by small lenders – needs in order to achieve the complicated balance between innovation, financial system stability and access to finance.

On the other hand, regarding payment services providers, regulators need to think about that in most jurisdictions they are not regulated under the same rules than traditional financial institutions, and accordingly, they do not have access to liquidity management support. In India, for example, service providers are incurring in additional cost related to liquidity management due to the upsurge in cash-out transactions in rural areas. Several factors have made rebalancing cash difficult. These include the sudden demand for cash, restrictions on movement and long distances to cover. The distance to bank branches that are often as far as 10-12 kilometers, and shutting down of public transport, and lack of personal transport options for agents make thing even harder. Agents have even reported reducing their investment in liquidity to use the money and feed their families.[426]

Regulating the looming threat of digital lending platforms: New-gen loan sharks?

Digital lending platforms could help a lot in the post-pandemic world. However, evidence and recent experiences in some jurisdictions such as India, Phillipines, and some African countries, show that desperate times make people vulnerable. In some countries, digital lenders are characterised for doing very quick disbursal of loans.[427] However, are changing high interest rates and performing practices that make people dependent on these platforms. In the post-pandemic, regulators need to diligently deter these practices. There are thousands of customers worldwide who have fallen prey to such lending platforms which are misusing data, overcharging customers and taking advantage of the digital illiteracy.[428] If not adequately address, financial inclusion can have a dark side.

From open banking to open data[429]

[...] Open banking initiatives, such as the use of Application Programming Interface (API) for data sharing in the post-pandemic world can be crucial to boost lending to the real economy. However, the current regulatory models that target open banking might fall short to address the

[423] Todd H Baker and Kathryn Judge, 'How to Help Small Businesses Survive COVID-19' (2020) 620 Columbia Law and Economics Working Paper <https://papers.ssrn.com/abstract=3571460> accessed 8 January 2021.
[424] Baker and Judge (n 423).
[425] Baker and Judge (n 423).
[426] Narain and others (n 231).
[427] Prabhu Mallikarjunan, 'How App-Based Lenders Are Harassing, Sucking Borrowers Dry' (*The Federal*, 11 June 2020) <https://thefederal.com/the-eighth-column/how-app-based-lenders-are-harassing-sucking-borrowers-dry/> accessed 8 January 2021.
[428] Mallikarjunan (n 427).
[429] Header from original paper.

post-pandemic challenges. Rather, shifting from open banking to *open data* and using open APIs not only to expose data collected by banks, but also data from other data sources (contextual accounting data, supply chain data and transactional data), This will facilitate sound lending decisions to help the real economy by developing new products driven by data and built around the SME's dynamic credit requirements after COVID-19.[430]

Data challenges for regulatory agencies[431]

As fintech transforms the financial sector, it also opens up data gaps in central bank statistics. It does so by introducing new financial products, and bringing existing services to a larger market. Data gaps are currently prevalent as (internationally comparable) information on fintech is lacking in official statistics. To understand innovation, qualitative information, information on evolving structures, and harmonised time series are needed.[432]

In the post-pandemic world, central banks and financial regulators will need to close this gap and develop a comprehensive process to continuously monitor the situation and address fintech-related data issues that may arise.

The role of standard setting bodies[433]

Fintech and, therefore, data-driven innovations in the financial sector exacerbate the difficulties of standard setting in international financial regulation.[434] Reliance on automation and artificial intelligence, novel types of big data, as well as the use of disintermediating financial supply chains, the interconnectedness with technology companies and third party services providers, complicate the balancing of different regulatory objectives.[435]

In the post-pandemic world, this challenge might be exacerbated. Innovative algorithms will introduce informational uncertainties and complex risks for market integrity. Further, regulation's ability to impose compliance costs on firms in response to these risks is limited when a preference for innovation favors smaller upstarts and non-traditional players.[436] International debate is much needed in this space in order to prevent a financial crisis derived from exacerbated risks, especially considering that in the post-pandemic data-driven finance will no longer be an innovation, but a mainstream development. ***[Financial System paper]***

[430] For more about the concepts of open banking and open data see Remolina (n 244).
[431] Header from original paper.
[432] 'Towards Monitoring Financial Innovation in Central Bank Statistics' (2020) IFC Report No 12 Bank for International Settlements <https://www.bis.org/ifc/publ/ifc_report_monitoring_financial_innovation.pdf>.
[433] Header from original paper.
[434] Yesha Yadav, 'Fintech and International Financial Regulation' (2020) 53 Vanderbilt Journal of Transnational Law 1109.
[435] Brummer and Yadav (n 243).
[436] Yadav (n 434).

6. Predicting upcoming challenges

At the time when the Centre's research papers were written, several authors had postulated some of the upcoming challenges and problems that were predicted to surface in the months after their papers were written. The following section explores three main immediate challenges that regulatory bodies and authorities must be cognizant of and prepare for: the rise of immunity passports, vaccine access and fair distribution, and limiting the extent of expanded surveillance, bearing in mind issues relating to post-crisis retention and use of personal data.

6.1 The rise of immunity passports

In efforts to return to a pre-pandemic state of normality, States are looking into the possibility of implementing "immunity passports" as an attempt to moderate and ensure the safe resumption of work in physical spaces and global travels. The excerpts below explore potential ramifications that may result from the use of this measure.

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,[437] and based on immunity status, issue an "immunity passports".[438] 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.[439] China is presently implementing a less hard-edged scheme where individuals seeking to travel in the country must obtain and display a health certification certificate, on their mobile devices.[440] ***[Covid Regulation paper]***

~

[437] 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.

[438] 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.

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

[440] 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 24 June 2020.

So far governments and private organisations working on these segregation initiatives do not appear to be addressing the challenges related to discrimination, fairness or even if these initiatives would be constitutional or in violation of international human rights instruments. Against any confidence in such segregation initiatives, the World Health Organisation has stated that there is no sufficient evidence about the effectiveness of antibody-mediated immunity to guarantee the accuracy of an "immunity passport" or "risk-free certificate."[441] People who assume that they are immune to a second infection because they have received a positive test result may ignore public health advice at other levels and thereby engage in more risky behaviours on the assumption that they cannot be re-infected. The use of such certificates could therefore increase rather than guard against the propensity for continued transmission. As new evidence becomes available, the World Health Organisation will update their statement on anti-body protections.[442] Nonetheless, organisations and governments progress with immunity passports. ***[Ethics paper]***

6.2 Vaccine access and fair distribution

Alongside issues of immunity passports, another ongoing challenge that authorities need to pay close attention to is anticipating and preparing for equitable vaccine access and distribution. The section below analyses the kinds of impact that intellectual property rights regimes may have on vaccine distribution, and emphasises the need for international regulatory cooperation in light of potentially defensive practices.

A note on this subsection: Excerpts submitted in this chapter were written during the earlier phase of the pandemic (in June 2020) and prior to the discovery of a vaccine. Nonetheless, we have opted to include this information to invite readers to consider the impact of intellectual property regimes on current vaccine distribution and delivery, including the need for regulatory refinement and a global approach to eliminating health inequalities.

The fallout from COVID-19 has culminated in an ongoing global race amongst laboratories to develop an efficacious yet safe vaccine in order to stem the damage caused by COVID-19. An efficacious yet safe vaccine, once administered to sufficient numbers in a country's population, will allow a country to move towards herd immunity.[443] If and when herd immunity is achieved, a country would be able to ease any existing distancing and quarantine measures put in place and allow more engaged economic activities to resume without having to unnecessarily endanger their healthcare system's capacity in doing so via risking successive waves of infection. (...)

There is little doubt that with a health and safety control environment currently largely located in nation state policy and fragmented national self-interest, the global co-operation in genetic sharing and collaborative immunological research, makes the vaccine quest unique in this pandemic eradication struggle. That said, there is mounting concern that without major philanthropic investment, the roll out of a vaccine may see a return to parochiality and hegemonic discrimination. (...)

---

[441] '"Immunity Passports" in the Context of COVID-19' (n 440).
[442] '"Immunity Passports" in the Context of COVID-19' (n 440).
[443] 'Herd Immunity and COVID-19 (Coronavirus): What You Need to Know' (*Mayo Clinic*, 6 June 2020) <https://www.mayoclinic.org/diseases-conditions/coronavirus/in-depth/herd-immunity-and-coronavirus/art-20486808> accessed 23 June 2020.

The paper speculates on the role of regulation, and particularly law in clarifying the access agenda and ensuring just and fair availability of whatever protection a vaccine can provide is not purely predicated on market forces. (...)

Accepting that substantive IP rights on their own are not to blame for adverse access outcomes, the need for compulsory licences and TRIPS exceptions reveals that a state cannot rely on the good intentions of successful manufacturers to promote social good when profits are potentially significant and market competition is constrained. Sustainable markets for life-saving medications are not only a matter of money. The political, economic, hegemonic and social externalities pressuring for more socially responsible commercial decision-making in this vaccine development context are unique but even so law's normative framework for justice and fairness is a powerful counterbalance to private property exclusion when world health is at stake. (...)

Bearing in mind the health and economic destruction caused by COVID-19, there may be concerns that governmental regulations may pose impediments in the timely approval of a vaccine for COVID-19 upon the successful conclusion of clinical trials. This would then potentially lead to either delays in vaccine availability and/or drive the costs of the successful vaccine higher if the production process was burdened with additional compliance costs, and competitive edge sacrificed through non-uniform national regulatory regimes. (...)

With every passing day that a successful vaccine is not distributed, billions of dollars in terms of economic damage is caused due to the restrictions on commerce and business which distancing measures and impediments of open borders/free movement produce. The spread of the pandemic is evidence enough that we live in an inevitably interconnected world. No national economy is immunised against the shocks caused to global trade and cross-border supply chains. Under such circumstances, perhaps, any concern should lie in the possibility that there may be insufficient regulation as regards the safety of the use of the "successful vaccine" with the general population when roll out is driven by economic imperatives rather than regulatory prudence. Unlike any other health crisis in living memory, because of its infectious spread and the unusual reality that morbidity is not largely over-represented in small and medium income economies, the desire for vaccine protection is now also a powerful political agenda. In this atmosphere of desperation, it is difficult to represent regulatory caution as anything more than another impediment to returning to some *new normal*. As has been witnessed in the rush to rely on digital tracing apps, with their operational limitations and attendant public opposition, as a means of getting people back to work, the regulatory parameters are no longer objectively or scientifically dispassionate. One needs no better evidence than the funding conditions exacted by Operation Warp Speed – millions of first preference doses going to the donor state before the market has a measure. The counter argument is that without preferential access sponsorship may not be forthcoming and this would have a more wide-spread disadvantage. Even so, this preferential approach reveals the fallacy in raising patent registration as the primary impediment to universal access at the earliest opportunity, if this is defined as a just and fair outcome. (...)

[...] There may be some concerns that intellectual property rights, in particular, patents, may pose an impediment to access to the successful vaccine.

In the context of this vaccine development, the discussion of the law's protectionist potential through exclusionist property rights can no longer be divorced from wider concerns of social

good.[444] (...) The race for a vaccine has demonstrated pre-considerations of state reputational value and parochial national interests. Thus, whether a nation state is minded to resist the patent application, through narrowly interpreting the application requirements and implicitly preferring more open market access, in the current political and economic pressure-cooker, a COVID-19 vaccine will certainly not escape social good evaluation or considerations of national economic and social priority. While patentability is a legal determination, the agents of the law do not operate in a vacuum and as with compulsory licensing, the consideration of how requirements will be fulfilled (in common law at least) does not escape appreciations of normative principle. (...)

In the event that a patent owner is determined to exploit and/or enforce his rights under the patent(s) conferred in relation to the successful vaccine, this would nevertheless not pose an impossible impediment to access to the successful vaccine.

As Francis Gurry, the director-general of WIPO, argued recently in relation to COVID-19: "The IP system recognizes at both the national and the international levels that emergencies and catastrophes may call for measures that may disrupt the normal functioning of the incentive framework upon which the IP system is based during the period of the emergency or catastrophe. The policy measures that are available in international and national IP law to manage and to mitigate emergencies and catastrophes include compulsory licenses and licenses of right of patented technology embodied in vital medical supplies and medicines… These measures, when deployed in a targeted and time-bound manner, may be useful or even vital when there is evidence of a need to which they may be addressed."[445]

Indeed, this is echoed in Art 8(1) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (hereinafter referred to as "the TRIPS Agreement"), which provides that: "Members may… adopt measures necessary to protect public health… and to promote the public interest in sectors of vital importance to their socio-economic and technological development." Art 8(1) TRIPS has been further affirmed by the World Trade Organisation's Doha Declaration on the TRIPS Agreement and Public Health, which states as such at paragraph 4: "The TRIPS Agreement does not and should not prevent Members from taking measures to protect public health. Accordingly, while reiterating our commitment to the TRIPS Agreement, we affirm that the Agreement can and should be interpreted and implemented in a manner supportive of WTO Members' right to protect public health and, in particular, to promote access to medicines for all."[446]

Therefore, countries can enact legislation or take necessary steps to effectively overcome any IP barriers (such as market price deflation) in ensuring access to crucial medicines/vaccines especially during a pandemic. One such way is through compulsory licensing. Compulsory licensing refers to a:

> "mechanism for superseding the exclusivity associated with patents in case of failure on the part of the patent owner to perform his obligations. It is a system whereby the government or government agency allows third parties (other than the patent holder, typically the competitor) to produce and market a patented product or process without

[444] Findlay (n 197).
[445] Francis Gurry, 'Some Considerations on Intellectual Property, Innovation, Access and COVID-19' (*World Intellectual Property Organisation*, 24 April 2020) <https://www.wipo.int/about-wipo/en/dg_gurry/news/2020/news_0025.html> accessed 24 June 2020.
[446] Elizabeth Siew Kuan Ng, 'Balancing Patents and Access to Medicine' (2009) 21 SAcLJ 457.

> the consent of the patent owner. This mechanism enables timely intervention by the government to achieve equilibrium between two objectives of rewarding inventions and in case of need, making them available to the public during the term of the patent. Through such an intervention mechanism, the government balances the rights of the patent holder with his obligations to ensure working of patents, availability of the products at a reasonable price, promotion and dissemination of technological invention, and protection of public health and nutrition."[447]

Most national legislations therefore allow for compulsory licences to be granted, which generally "compels the pharmaceutical company to grant a licence to another company (usually a generic drug company) upon terms (including royalty) to be agreed by the pharmaceutical company and the other company; or, failing agreement, determined by the court."[448]

Taking India as an example, the grounds for granting a compulsory licence are provided for under s84(1) of the Indian Patents Act 1970. These are, namely: (a) that the reasonable requirements of the public with respect to the patented invention have not been satisfied (s84(1)(a) Indian Patents Act 1970), or (b) that the patented invention is not available to the public at a reasonably affordable price (s84(1)(b) Indian Patents Act 1970), or (c) that the patented invention is not worked in the territory of India (s84(1)(c) Indian Patents Act 1970). To succeed, the applicant for a compulsory licence must establish at least one of these grounds.

The Indian Controller of Patents and Designs issued a compulsory licence in the decision of *Natco Pharma v Bayer Corp.*[449] The patent in dispute concerned Nexavar, a drug used to treat renal cell carcinoma and hepatocellular carcinoma and the patent thereof was owned by Bayer Corp. The Controller granted a compulsory licence under all three grounds in s84(1) of the Indian Patents Act 1970, holding that "(a) Bayer had made its drug available to only a small percentage of eligible patients, which did not meet the reasonable requirements of the public; (b) the price of close to rupees 280,000/- per month was not reasonably affordable to the purchasing public; and (c) Bayer's patent was not being worked in India as Nexavar was not being manufactured in India."[450]

Therefore, with a robust compulsory licensing framework under national legislations, as permitted under the TRIPS Agreement during a health crisis, "it would be inaccurate to blame any problems in accessing a vaccine on the global IP system."[451] Any successful manufacturer who files a patent and intend to reap massive profits would quite likely anticipate compulsory licenses to be taken out against them.

Despite the paper's confidence in IP not being the exclusionist regime which will retard vaccine access, compulsory licences have been developed to prevent just that outcome. It is a truism to say the law in substance cannot be blamed for the exploitative intentions of those to whom it grants rights. However, compulsory licences and deflated market pricing regimes, as well as the TRIPS exceptions referred to above, are evidence that IP rights protections can prefer

---

[447] Reto M Hilty and Kung-Chung Liu, *Compulsory Licensing: Practical Experiences and Ways Forward*, vol 22 (Springer 2015) 12.
[448] Tee Jim Tan, 'Will Global IP System Block Access to Vaccine?' *The Straits Times* (28 May 2020) <https://www.straitstimes.com/opinion/will-global-ip-system-block-access-to-vaccine> accessed 24 June 2020.
[449] Bayer Corporation v. Union of India, The Controller of Patents and Natco Pharma Limited, MANU/IC/0016/2013
[450] Hilty and Liu (n 447) 21–22.
[451] Tan (n 448).

individual rather than social interests, particularly where the health of the globe is at stake, and without these alternative measures, social good may not be achieved. IP law offers choices to successful manufacturers that might bring about high market pricing to the disadvantage of many consumers. Compulsory licences are a device available to the state (and the market) to modify the exclusionist impact of royalty pricing. Again, we return to the consideration of manufacturer's choice enabled through law but moderated either by market intervention or (as is the case with the current pandemic) influential political, hegemonic, economic and social externalities. In such considerations law's strong normative framework which is equal to claims for private property endorsement at the high a cost of equality before the law, should be recalled in debating law's regulatory function, as much as is the substantive property rights options the law offers.[452] (...)

History has shown that private sector initiatives and global collaboration efforts had similarly ensured access to vital vaccines and medicines. One such example can be seen in Unitaid, which is an international organisation working in collaboration with the WHO and "invests in innovations to prevent, diagnose and treat HIV/AIDS, tuberculosis and malaria more quickly, affordably and effectively" and also "work to improve access to diagnostics and treatment for HIV co-infections such as hepatitis C and human papillomavirus".[453]

One of the initiatives under Unitaid is known as the "Medicines Patent Pool". As explained above, a patent owner has no legal obligation to exploit his patent, but the rights conferred to him under a patent nevertheless allows him to seek injunctive relief and damages against an infringer. The Medicines Patent Pool negotiates voluntary licences with pharmaceutical companies on behalf of middle-and low-income countries. Under such voluntary licences, the patent owner may permit certain generics to manufacture and sell the patented drug or vaccine under negotiated terms and conditions. Such terms and conditions may, for example, limit the generics in terms of the quantities of the patented drug or vaccine which it may be permitted to produce, stipulate whether royalties are payable and to whom the generics can supply the patented drug or vaccine, etc.[454] Such a voluntary patent licensing pool scheme had been shown to succeed in "lowering prices and ensuring fair and equitable distribution of the medicines relating to those diseases to poor countries."[455]

Specifically, in the context of COVID-19, pharmaceutical companies such as Johnson & Johnson (which is receiving support from the US Government under Operation Warp Speed) has pledged its commitment "to bringing an affordable vaccine to the public on a not-for-profit basis for emergency pandemic use."[456] Alex Gorsky, CEO of Johnson & Johnson, said in this regard: "The world is facing an urgent public health crisis and we are committed to doing our part to make a COVID-19 vaccine available and affordable globally as quickly as possible. As

---

[452] Randall Peerenboom, 'Human Rights and Rule of Law: What's the Relationship?' (2005) 36 Georgetown Journal of International Law <https://papers.ssrn.com/abstract=816024> accessed 7 January 2021; Oona A Hathaway, 'Do Human Rights Treaties Make a Difference?' (2002) 111 The Yale Law Journal 1935.
[453] 'About Us' (*Unitaid*) <https://unitaid.org/about-us/> accessed 25 June 2020.
[454] 'Unitaid's Approach to Intellectual Property' (Unitaid 2016) <http://unitaid.org/assets/Unitaids-approach-to-intellectual-property.pdf> accessed 24 June 2020.
[455] Tan (n 448).
[456] 'Johnson & Johnson Announces a Lead Vaccine Candidate for COVID-19; Landmark New Partnership with U.S. Department of Health & Human Services; and Commitment to Supply One Billion Vaccines Worldwide for Emergency Pandemic Use | Johnson & Johnson' (*Johnson & Johnson*, 30 March 2020) <https://www.jnj.com/johnson-johnson-announces-a-lead-vaccine-candidate-for-covid-19-landmark-new-partnership-with-u-s-department-of-health-human-services-and-commitment-to-supply-one-billion-vaccines-worldwide-for-emergency-pandemic-use> accessed 24 June 2020.

the world's largest healthcare company, we feel a deep responsibility to improve the health of people around the world every day."[457] Other private sector initiatives, such as the collaboration between Gavi and the Bill & Melinda Gates Foundation, have pledged "to purchase COVID-19 vaccines for lower-income countries as soon as they are available."[458]

Again, this is a situation where the conciliatory intervention of 'honest brokers' has ameliorated the royalty impact of patent rights enforcement, particularly when some countries cannot meet the protected market price. In his seminal work on the pharmaceutical industry John Braithwaite not only indicates how the protection of patent rights can reduce market competition and increase consumer pricing, but exposes how assurances from these rights holders that they will 'do the right thing' need at least the counterbalance of community debate, civil society scrutiny and a strong humanitarian counter-movement.[459] (...)

Successful vaccine or not, it would be negligent either to relax regulation on its promise, so the limitations of any panacea are not to the fore, and the negative side-effects (if any) are known for informed patient choice. ***[Vaccine paper]***

~

The greatest accessibility issue at the centre of alleviating the crisis is vaccine availability and coverage. China has pledged a massive manufacturing capacity to make available vaccine advantage world-wide.[460] 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.[461] One of these organisations at least has promised to charge out doses at cost for the life of the pandemic.[462] 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.[463] Social justice over profit protection is recognised in international trading agreements for circumstances such as these.[464] ***[Covid Regulation paper]***

---

[457] 'Johnson & Johnson Announces a Lead Vaccine Candidate for COVID-19; Landmark New Partnership with U.S. Department of Health & Human Services; and Commitment to Supply One Billion Vaccines Worldwide for Emergency Pandemic Use | Johnson & Johnson' (n 456).

[458] Bill Gates, 'When a COVID-19 Vaccine Is Ready, This Group Will Make Sure the Whole World Can Access It' (*Bill & Melinda Gates Foundation*) <https://ww2.gatesfoundation.org/ideas/articles/coronavirus-gavi> accessed 24 June 2020.

[459] John Braithwaite, *Corporate Crime in the Pharmaceutical Industry* (Routledge 2013).

[460] 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.

[461] Ara Darzi, 'The Race to Find a Coronavirus Treatment Has One Major Obstacle: Big Pharma' *The Guardian* (2 April 2020) <http://www.theguardian.com/commentisfree/2020/apr/02/coronavirus-vaccine-big-pharma-data> accessed 20 May 2020.

[462] Zia Sherrell, 'Experts Weigh in on How Much a Dose of a Successful Coronavirus Vaccine Could Cost' *Business Insider* (5 May 2020) <https://www.businessinsider.com/how-much-will-coronavirus-vaccine-cost-2020-5> accessed 20 May 2020.

[463] Sherrell (n 462).

[464] David P Fidler, 'Negotiating Equitable Access to Influenza Vaccines: Global Health Diplomacy and the Controversies Surrounding Avian Influenza H5N1 and Pandemic Influenza H1N1' (2010) 7 PLOS Medicine e1000247.

6.3 Extended and expanded surveillance including post-crisis retention and use of personal data

Finally, as discussed in section 3.3, there is a growing worry that the increased pervasive surveillance measures, along with all the associated data collected, will be a permanent fixture within society. Wee and Findlay highlight the implications of prolonged and indefinite use of surveillance and its effect on citizen distrust, and draw on existing critique on the implementation of sunset clauses. These concerns cannot be shirked aside or dealt with at a more convenient time, for they must be continually at the forefront of the minds of State authorities, as the pandemic continues to ravage the world.

One of the ways which the discussion can contribute to the literature is by highlighting the harms of governments building surveillance infrastructures to combat COVID-19 or adapting pre-existing technological potential, which then remain around for purposes other than COVID-19 after the pandemic is over. One such example (albeit not in relation to a pandemic) would be that of the 9/11 terrorist attack where the US government created "new surveillance infrastructure [that] gave more power to the very institutions whose failure created the crisis."[465] The American Bar Association argues that:

> [p]rivacy rights… have been eroded because, in the wake of 9/11, Congress dismantled the "wall" between government surveillance for domestic law enforcement purposes and surveillance activities for foreign-intelligence gathering.[466] ***[Ethics paper]***

~

Duration of retention of data[467]

Despite calls for deletion of data after it has fulfilled its health protection purpose,[468] this has not prevented governments from justifying permanent retention,[469] as was the case in South Korea which sought to permanently retain health data after the MERS outbreak ended.[470]

To alleviate the public's worries in this regard, experts have advised that governments must clearly explain their intended data use, and the measures that are in place to secure such data. This invocation is particularly important in countries like Singapore, since the Personal Data Protection Act 2012[471] applies to individuals and business organisations and not to the

[465] Henry de Valence, 'Let's Develop Decentralized, Privacy-Preserving Contact Tracing' (*The Zcash Foundation*, 23 March 2020) <https://www.zfnd.org/blog/decentralized-contact-tracing/> accessed 30 March 2020.
[466] Hina Shamsi and Alex Abdo, 'Privacy and Surveillance Post-9/11' [2011] American Bar Association <https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/> accessed 31 March 2020.
[467] Header from original paper.
[468] Samuel Stolton, 'Vestager: It's Not a Choice between Fighting the Virus and Protecting Privacy' (*www.euractiv.com*, 17 April 2020) <https://www.euractiv.com/section/digital/news/vestager-its-not-a-choice-between-fighting-the-virus-and-protecting-privacy/> accessed 19 August 2020.
[469] 'Privacy vs. Pandemic Control in South Korea' (n 88).
[470] 'South Korea Admits Keeping Personal Data Of 2015 MERS Outbreak Patients' (*NPR.org*) <https://www.npr.org/2020/06/23/882481377/south-korea-admits-keeping-personal-data-of-2015-mers-outbreak-patients> accessed 5 August 2020.
[471] 'Personal Data Protection Act 2012 - Singapore Statutes Online' (n 79).

government.[472] Without having insights to the internal guidelines that govern state agencies, the public remains unaware of the rules that public bodies follow beyond assurances made by ministers. This may impede incentives to trust that data use and retention will be handled properly by state agencies. The onus lies on the government to manage data responsibly and address significant queries, and to do so with informed public trust and confidence at the forefront of their response efficacy policy. (...)

Justification for greater surveillance in the future[473]

Another thread of disquiet centres on the long-term political and legislative impacts of enhanced surveillance. Many of the technologies employed in COVID-19 control surveillance systems were already in place prior to the pandemic. A cursory scan of these established frameworks, particularly in global cities, demonstrates the extent of invasive surveillance that data subjects are already under. For instance, China utilises its pre-existing wide-scale facial recognition technology to monitor the movements of its citizens in assessing whether stay-home orders are being breached,[474] and thermal scanners now display commuters' infrared images in train stations.[475] Among the Chinese citizenry, the use of such technologies appears to be not only tolerated, but accepted, understood, and even gaining popularity as necessary control responses. It might be speculated that such community compliance in an authoritarian administration where surveillance intrusions have become a common feature of daily life, and dissent against the state is not welcomed, could be anticipated. Even so, there have been isolated expressions of unease, where activists and dissidents have been detained under the guise of quarantine.[476] Israel is another jurisdiction where surveillance is well-developed, and the citizens are used to comprehensive national security measures. The state utilises phone and credit card data to map the movement of the virus, alerting and quarantining individuals who had come into close contact with confirmed patients.[477] In Russia, the Moscow police has been experimenting with a host of surveillance technologies by monitoring data subjects' social networks and geolocations, and have most recently claimed that the use of a 170,000-camera facial-recognition system effectively helped them catch and fine over 200 people who violated quarantine and self-isolation.[478]

From the above discussed expansive surveillance regimes, the question arises whether these surveillance technologies expanded in the pandemic context, will be further normalised as the public becomes less sensitive to privacy infringements and, consequently, less resistant to *even* greater intrusion in the name of public safety (argued as necessary for an eventual return to a less rights-restricting life).[479]

---

[472] Currently, the government's data sharing protocol is governed broadly by the Public Sector Governance Act. See 'Public Sector (Governance) Act 2018 - Singapore Statutes Online' <https://sso.agc.gov.sg/Acts-Supp/5-2018/Published/20180305?DocDate=20180305> accessed 4 August 2020.
[473] Header from original paper.
[474] 'Coronavirus Brings China's Surveillance State out of the Shadows' (n 7).
[475] April 25th and others, 'Covid-19: The Controversial Role of Big Tech in Digital Surveillance' (*LSE Business Review*, 25 April 2020) <https://blogs.lse.ac.uk/businessreview/2020/04/25/covid-19-the-controversial-role-of-big-tech-in-digital-surveillance/> accessed 20 July 2020.
[476] Sui-Lee Wee, 'China Uses Quarantines as Cover to Detain Dissidents, Activists Say' *The New York Times* (30 July 2020) <https://www.nytimes.com/2020/07/30/world/asia/coronavirus-china-quarantine.html> accessed 6 August 2020.
[477] CNN (n 91).
[478] CNN (n 91).
[479] Motsenok and others (n 6).

As with pandemics of this magnitude, the demarcation between emergency and new normalcy is far less distinct than conventionally envisioned in lesser health crises, and currently there is no determinative marker signalling an appropriate time in which these strict measures ought to be lifted. Undeniably, the illusory finishing line of this pandemic underscores the rationale for extending rights-restricting measures in control policies, further entrenching the surveillance regime within society. Ultimately, the longer such AI-assisted surveillance technologies are accessible and proliferate in society; the easier it is to ignore their medium-term reach, and to become resigned to the compromise of rights and liberties, forget the disquiet that emerged in the initial stages of the control responses. Bearing this in mind, there is a responsibility on surveillance technology promoters to build in regulatory protections (ethical compliance in particular) at all stages of implementation and operation.[480]

Retention of mass surveillance post-pandemic[481]

The extent of surveillance, in terms of coverage and depth of intrusion, justified by a foreseeable diminution of the pandemic threat, belies the difficulty in any incremental reduction in crisis justifications for mass surveillance data collection.[482] Presently, states justify the need for biometric surveillance in order to prevent further waves of virus or a new strains of infectious disease.[483] That said, state agencies may maintain the heightened levels of surveillance post-pandemic rather than reckoning with difficulties in scaling down their activities.[484] Besides community opposition and dissent from pressure groups, there will be no real incentive for the state to reduce the levels of surveillance, particularly with technology in place, and its potentially diversified application of surveillance data beyond pandemic control continuing unaddressed.

To allow the continuation of an aggressive, unchecked expansion of surveillance programs could lead to a reality of normalised privacy intrusions, which may potentially be used for political repression.[485] In this respect, community disaffection and pressure for inclusion and monitoring provides important checks and balances over a surveillance society future.

Utility of implementing sunset clauses[486]

In the face of intrusive short-term measures, a commonly exercised legislative tool is the introduction of sunset clauses necessitating a return to some power status quo as the pandemic winds down. When the public believes that such invasive measures will eventually discontinue, it may be more are willing to endure a temporary curtailment of rights and rationalise the surveillance regimes as being a necessary and perhaps proportionate response to resolve the immediate health crisis.[487] However, any normalisation of such surveillance technologies bringing with it feelings of inevitability and resolve, can have a muting effect on public opposition and the revaluing of liberty and individual dignity.

---

[480] Findlay and Remolina (n 57).
[481] Header from original paper.
[482] 'Should I Worry about Mass Surveillance Due to COVID-19?' (n 161).
[483] Wim Naudé, 'Artificial Intelligence vs COVID-19: Limitations, Constraints and Pitfalls' [2020] Ai & Society 1.
[484] Kharpal (n 58).
[485] 'How to Protect Both Public Health and Privacy' (*Freedom House*) <https://freedomhouse.org/article/how-protect-both-public-health-and-privacy> accessed 30 July 2020.
[486] Header from original paper.
[487] Sharon (n 61).

The prevalence and pervasiveness of individual surveillance has spill over effect into other contemporaneous control and social order policymaking which may have long-term consequences. For instance, Motsenok et al. argue that the unintended consequence of sunset clauses creates a termination paradox, as temporary measures, so moderated with expiry dates, may, invariably lead to a proliferation of control policies that would not otherwise have been approved.[488]

The absence of a general discussion about phasing down surveillance and the expiration of COVID control data cannot simply be explained away by uncertainty regarding the evolution and containment of the virus. As was mentioned earlier there has been critical debate about the necessary inclusion in emergency powers legislation, or specific COVID-19 control provisions, of sunset clauses in the legislation.489 This discussion has not been matched by energetic and detailed exploration of phasing out emergency powers and timetables for surveillance technology demobbing and data expiration. The phased destruction of pandemic-related data and decommissioning of surveillance capacity would be a tangible feature, and an empirically measurable confirmation, of any return to normality. If this is to be qualified by an ongoing need to prepare for another pandemic, then the technology and its data can be mothballed until the emergency signs reappear. With the experience gained in this pandemic control exercise, the recommissioning of technology will not be an obstacle to responsible pre-pandemic preparation. [Disquiet paper]

[488] Marina Motsenok and others, 'The Slippery Slope of Rights-Restricting Temporary Measures: An Experimental Analysis' [2020] Behavioural Public Policy 1.
[489] 'Second Reading Speech by Senior Minister of State for Law, Mr Edwin Tong, on the COVID-19 (Temporary Measures) Bill 2020' <https://www.mlaw.gov.sg/news/parliamentary-speeches/Second-Reading-Speech-by-Senior-Minister-of-State-for-Law-Mr-Edwin-Tong-on-the-COVID-19-Temporary-Measures-Bill-2020> accessed 4 August 2020.

7. A global approach

Reflections from the Centre's Director, Prof Mark Findlay

The extracted material that has gone before evidences anything but a global approach to pandemic control. This has not just been a story of blatant national interest (although recent experiences of *vaccine politics* suggest ample emphasis on that). The North/South world divide stands apparent. Reverting to vaccines, the North world invents and develops the drug, the South world often manufactures the doses, the North world is first advantaged through inoculation, and then the debate rages about whether more equitable access to the science should be a matter of charity or knowledge sharing. The short-sightedness of this duality in equitable access, and the need for global solutions is clear while the rest of the world waits on vaccination as virus variants continue to mutate that will challenge even those who have had their shots in the more developed nations.

Populist politics has added to the confusion over a global approach to pandemic control. Borders are closed to keep out foreign infections, then opened to attract tourist dollars. Recriminations rage around where the pandemic originated and which country bears responsibility, while international health organisations are pilloried for partiality, and funding is strangled away from resourcing global health protection. Populists deny the pandemic and the utility of vaccination when it is abundantly on offer and the medical evidence point in support of prophylactic approaches. This debate is happening at the same time where more than 70% of the world's population does not have the perverse luxury of such a choice.

When a global approach to pandemic control (or its failure) is under consideration, two general considerations arise from our research that are significant:

1. What does it mean to be a global citizen?
2. Where should the global citizen be positioned when technology and mass data sharing are prominent control policies?

The first question is too broad and contentious to receive adequate treatment here. Suffice to say that when confronted by imminent and encompassing global crises, political, economic, racial, social, historical and hegemonic discriminators carry less weight. How often has it been said that when it comes to infection COVID-19 knows no borders and does not account for the identifiers just mentioned? If this is so, then the global citizen facing global crises, is not to be understood in the exclusionist manner in which we understand national citizenship. Citizens in a globalized world with a largely digital existence no longer relate to space and time as might be expected before the Internet. Globalisation is the method and the process for interconnected world communication. Anxiety and protectionism are its foes. Global citizens will only exercise the potential that globalisation offers for humanity in communal rather than individualist identities if trusted relationships replace distrusting animosities. Unfortunately, the egoist survivalism predisposition which has been a feature of national responses to this pandemic does not encourage communitarian 'risk-to-fate' journeying. Neoliberal exclusionism, and individualist wealth creation before communal sustainability, which are features of the economy versus health trade-off bogging down collective pandemic containment, foreshadow not just a prolonged disruption of social bonding but an unpreparedness to address the monumental global challenges to come.

A recurrent theme in the research summarised in this compendium is the significance of trust for both control efficacy and citizen engagement. The nationalist and populist responses to the pandemic are anything but reflective of shared trust and communal responsibility.

Globalisation has in the mind of many been equated with the problem and not the solution to such a global crisis. True it is that one thing distinguishing this plague epoch from comparable emergencies in the past is the massive physical and digital interconnectedness of the planet. However, while this might explain the spread of the virus it can also offer hope for shared control and containment strategies.

As a sad consequence of populist politics and neoliberal individualism, globalism is again on the receiving-end of blame as the pandemic rages. We know that unlike pandemics gone by, porous borders and international travel have fuelled the spread of this disease. It is such openness of movement, and cross-border engagement politically, culturally, socially and economically that have become casualties to jurisdictionally-centred and motivated control responses.[490] At a moment in history when we need a global strategy for a global problem, instead we have accusations of cyber-attacks on vaccine research facilities, and the rich nations colluding with big pharma to stockpile doses and offer preferential roll out. A global initiative for universal inoculation, instead of seeming a natural coalition, has been a tortuous path of bargaining self-interest and hegemonic imperialism.

The dangerous diminution of human interconnectedness by populist exclusionism should be condemned by every responsible world leader and commercial magnate. The false choice between economic recovery and human-centred pandemic control conventions needs to be called out. The campaign for individualist liberties which has little or no concern for responsible communal obligations should be exposed as an egoist dereliction and not a struggle for constitutional rights. Yet as the current reluctance of major social media platforms in challenging and deactivating fictitious political propaganda about pandemic fantasies confirms, neoliberal exceptionalism can capture communication pathways for its own false messages, as easily as it has perverted globalisation to its exclusive economic benefit.

Belief in shared communication pathways as alternative journeys to destructive self-interest is not misplaced, even though examples of miscommunication across global message platforms abound. Voices of the dispossessed, recurrent in the research above, are not blanked out by anxiety governance, and a chanting chorus rejecting a more universalised humanity.

The pandemic and looming climate change are finally shocking the otherwise-anxious into the realisation that what once was normal is no longer sustainable. If we are transiting into a 'post-normal' and 'post-human' world, like so many other *alter systems* projections, Luhmann would have considered these new eventualities as self-evident:

> ...the activity of expert advisers can no longer be adequately understood as the application of existing knowledge. While in communication, they have to withhold or at least water down uncertainties persisting in science, they have to avoid deciding political questions in advance as questions of knowledge. Their advice conveys not authority but uncertainty, with the consequence that the experts appear to be scientifically untrustworthy while presenting political politically inspired controversies

[490] COVID-19 control in federal systems such as the USA has become even more parochial as responsibility is passed to state, district and municipal authorities to differentially manage a disease with national and global reach.

> as differences in the assessment of scientific knowledge. As a result, they are likely to be regarded neither as scientists nor as politicians.[491]

Saul echoes these sentiments:

> The efficient delivery of indigestible quantities of information leaves the public little room to be more than a spectator. The rational advocacy of efficiency more often than not produces inefficiency. It concentrates on how things are done and loses track of why. It measures specific costs without understanding real costs. This obsession with linear efficiency is one of the causes of our unending economic crisis. Worst of all, it is capable of removing from democracy its greatest strength, the ability to act in a non-conventional manner, just as it removes from individuals their strength as non-linear beings.[492]

Answering the second question: where should the global citizen be positioned? No doubt the digitisation of social communication has taken over conventional systems of human intercourse and interaction. It is a moot question about the extent to which this will remain the case, once the pandemic crisis has been somehow normalised, particularly now that social distancing versus freedom of association has become such a cultural/political divide.[493] If health and safety common sense such as the wearing of masks and restrictions on association (advised by the WHO) continue to be portrayed as attacks on sovereignty and citizenship, safety through digitised communication will eventually also be targeted. It is clear in the citizen-centric theme that emerges from our work on distrust that social responsibility, rather than egoist individualism, is the only recipe for a global approach to crises such as this pandemic. Interestingly, when it comes to COVID-19 control, the libertarian lobby, conventionally opposed to universal rights assertions, are not above capturing this discourse when it opposes a communitarian approach to socially responsible self-determination.

[491] Niklas Luhmann, *Theory of Society, Volume 2* (Stanford University Press 2013) 114.
[492] John Ralston Saul, *Voltaire's Bastards: The Dictatorship of Reason in the West* (Simon and Schuster 2013) 582.
[493] Lisa Lerer, 'The New Culture War' *The New York Times* (7 May 2020) <https://www.nytimes.com/2020/05/07/us/politics/liberal-conservative-coronavirus.html> accessed 1 July 2021.

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Centre for
AI and Data Governance

Yong Pung How School of Law
Singapore Management University
55 Armenian Street
Singapore 179943

Website: caidg.smu.edu.sg

Enquiries: caidg@smu.edu.sg