AI AND DATA USE: SURVEILLANCE TECHNOLOGY AND COMMUNITY DISQUIET IN THE AGE OF COVID-19

Alicia Wee[1] and Mark Findlay[2]
Centre for AI and Data Governance, School of Law, Singapore Management University[3]

Abstract

The proliferation of surveillance technology during the COVID-19 pandemic has resulted in a myriad of responses from the public. This paper seeks to examine community disquiet in the context of these smart technologies. In particular, we look at 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 we 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". We find 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, we argue 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.

[1] Research Associate, Centre for AI and Data Governance, School of Law, Singapore Management University (email: aliciawee@smu.edu.sg). The authors are grateful for the invaluable comments and feedback from Jane Loo and Josephine Seah.

[2] Director of the Centre for AI and Data Governance, School of Law, Singapore Management University (email: markfindlay@smu.edu.sg).

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

Section 1: Introduction

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[4] 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.

This review cites disquiet surrounding surveillance strategies in various forms and degrees of intrusion. It unpacks the sources of disquiet and the specific foci of unease, more particularly than a general appreciation concerns for rights, liberties and normality. The endeavour to locate disquiet, understand its sources and emergence, realise what underpins these reactions and to progress a discussion of trust and efficacy, are the policy takeaways from what follows.

Due to the social realities of the pandemic and the diverse terrain over which disquiet manifests, we have not been able to institute original empirical research into public opinion. Even if that was possible, we know much disquiet grows from unfortunate ignorance fuelling negative perceptions of risk and unacceptable compromises. To ask citizens to rationalise their disquiet ignores the reality that through failures in public awareness promotion, stakeholders have been kept in the dark and left victims of populist conspiracy theorising and half-truths. We are a long way off from surveying a well-informed and considered debate about the pros and cons of trust formation or compliance withdrawal. That said, the expansive insights provided in what follows offer ample justification for promoting public awareness and community engagement as a policy priority preceding aspirations for control and prevention success.

1. The Purpose of this Review

Against the backdrop of differentially expressed but widely felt disquiet regarding AI-assisted control responses, this brief review presents three broad directions for the discussion to follow:

- To source and survey the discussions and debates concerning the implications of surveillance technologies on rights, liberties and integrity;
- To identify common themes in the concerns expressed; and
- To explore whether differences in social responses to surveillance controls are reflections of the authority that the state agencies are perceived to exhibit, the necessity of their operation in health/safety terms, and the extent to which the risks they pose to *individual* rights and liberties are not discounted against how *communities* value these rights and liberties.

[4] 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.

Citizen and community disquiet associated with AI-assisted COVID-19 control responses suggests two main analytical/policy purposes:

- Test the contention that the source of much disquiet is the failure of policymakers and technology advocates to adequately engage citizens and communities in the planning and implementation stages; and
- Evaluate if there is an apparent connection between disquiet, distrust and the overall effectiveness of these applications in achieving their control potentials.

Over the following sections, we chart the contextual relativity of reactions to intrusive control methods, the generation of community distrust as surveillance technologies produce and share massive amounts of personal data, and concerns about the longevity of such surveillance after the immediate pandemic justifications. Associated with these understandings are germs of deep confusion that range from the numbing effect of prevailing surveillance to the ways in which quite specific health/safety objectives are becoming blurred by increasing ancillary surveillance potential. The experiences documented in this report reveal that a core source of disquiet is the argument from proponents of these technologies – that civil liberties and data integrity are the necessary casualties of policies for a safer society.

Methodology

We examine various sources of texts (including social media posts, academic journals, app reviewers, and newspaper commentaries), and a wide range of active voices (including civil society groups, academics, researchers, user reviewers, etc.) expressing disquiet. For example, in section 2, we observed that human rights groups and civic activists had directly responded to officials, whether through social media or open letters, to raise privacy-related infringement concerns, inadequate transparency surrounding the app use, as well as data retention questions. We also examined surveys and peer-reviewed journal articles, echoing the sentiments of data subjects,[5] who share their legal and technical expertise to better situate the disquiet within the existing policy landscapes, along with its potential implications of inadequate control responses on public health and its citizens. The table in Section 3 is a collection of the different voices and the respective contentions experienced by data subjects in the pandemic. These categories are presented for the purposes of comparison, of which we are mindful that there are inevitable overlaps and interconnection across several categories.

Within this paper, the wide-ranging sources of disquiet appear to converge on the following concerns: frustrations associated with information deficits surrounding the operation and impacts of surveillance in order to evaluate their health and safety efficacy against their challenges to individual rights and liberties, and associated fears of over-surveillance by state and corporations ongoing. Inadequate community engagement in the roll-out of these technologies

[5] For the purposes of this paper, the term 'data subjects' refers to the wider public, civilians, and citizens who interact with the various sources of surveillance technology. 'Data subjects' is meant to encapsulate a diverse group of individuals who possess different degrees of technical knowhow and who have different levels of engagement with these technologies.

and insufficient participation offered to civil society in the oversight of the data that they provide seems to sit at the heart of public disquiet.

Although the responses are varied and heterogenous, this report is reliant on news reviews and academic commentary that largely drew information from big tech firms (e.g. Twitter) and data sharing conglomerates. We acknowledge that since our paper is informed by secondary materials, the tone of disquiet received may inadvertently be filtered through curated news content and other policy pronouncements which may not fully translate the embedded sentiments of data subjects. We intend to expand the scope of this paper to include empirical findings and primary research in future projects.

This paper is not intended to offer any evaluation of these control responses in terms of their purposes and objectives beyond reflecting on the reality: that for technologies which require citizen consent, compliance, voluntary uptake or general tolerance, distrust expressed in disquiet will have a negative influence on efficacy. It is necessary, therefore, to identify different sources of disquiet and discuss their potential implications and ramifications of these control responses.

2. Examining surveillance technologies during the COVID-19 pandemic

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,[6] GPS devices, and facial recognition technologies to permeate mundane situations of movement, association and daily social interaction.[7] 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.[8] 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.[9] Further, the recent global preference for ethics and principled design as sufficient regulatory frames for AI

[6] '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.

[7] Roberts (n 2).

[8] '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.

[9] For a detailed discussion of these challenges see, Mark James 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] SSRN Electronic Journal <https://www.ssrn.com/abstract=3592283> accessed 3 August 2020.

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.

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 just more of the same.[10] 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."[11] Recently in Singapore, police have pilot-tested automated drones to enforce social distancing measures in public spaces.[12] 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.[13]

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.[14]

[10] Marina Motsenok and others, 'The Slippery Slope of Rights-Restricting Temporary Measures: An Experimental Analysis' [2020] Behavioural Public Policy 1.

[11] '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.

[12] '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 6).

[13] '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; Sarah Boseley and Heather Stewart, 'Hancock: It Is Public's "civic Duty" to Follow Test-and-Trace Instructions in England' *The Guardian* (27 May 2020) <https://www.theguardian.com/world/2020/may/27/government-unveils-covid-19-test-and-trace-strategy-for-england> accessed 20 August 2020; 'Matt Hancock Says Public Has a "duty" to Download Coronavirus Contact Tracing App' (*Politics Home*, 5 May 2020) <https://www.politicshome.com/news/article/matt-hancock-says-public-have-a-duty-to-download-coronavirus-contact-tracing-app> accessed 20 August 2020.

[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.

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 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.[15]

[15] Mark Findlay and Nydia Remolina, 'Regulating Personal Data Usage in COVID-19 Control Conditions' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3607706 <https://papers.ssrn.com/abstract=3607706> accessed 4 August 2020.

Section 2: Main Themes

In this section we address major concerns raised by different communities. We have organised these concerns under the following six themes. Disquiet surrounding:

- the data collected;
- authority styles confirming control responses (external to the technologies employed);
- the internal architecture of control technologies employed;
- the infringement of rights and liberties;
- the role of the private sector in the pandemic; and
- uncertainties regarding the post-pandemic world and the "new normal".

1. Disquiet surrounding the data collected

(a) Safety, integrity, security, and storage of personal data

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,[16] who can *use and own* the data collected,[17] and for *how long* the data will be retained?

In Australia, the hybrid centralised/decentralised approach towards data collection has drawn criticisms from data subjects who are unconvinced that there is adequate protection of personal health data. Public discourse recalls violations of centralised databases as recent as 2016, during which the Australian government lost 2.9 million Australians' sensitive medical records due to "pure technical naivete".[18] More recently, there have been reported instances of hackers gaining access to, and leaking sensitive COVID-19 records, detailing more than 400 pages of communications and messages between health officials and doctors.[19] Experts have condemned

[16] 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.

[17] 'We Need Mass Surveillance to Fight Covid-19—but It Doesn't Have to Be Creepy' (*MIT Technology Review*) <https://www.technologyreview.com/2020/04/12/999186/covid-19-contact-tracing-surveillance-data-privacy-anonymity/> accessed 20 July 2020.

[18] 'What Price Privacy? Contact Tracing Apps to Combat Covid' <https://www.lowyinstitute.org/the-interpreter/what-price-privacy-contact-tracing-apps-combating-covid> accessed 5 August 2020.

[19] 'Hackers Leak Thousands of Sensitive WA COVID-19 Records Online' (*MSN*) <https://www.msn.com/en-au/news/australia/hackers-leak-thousands-of-sensitive-wa-covid-19-records-online/ar-BB16Xy49> accessed 5 August 2020.

the "unforgiveable" privacy breach and the ease of access to such sensitive health data,[20] given its potential for exploitation.[21]

Additionally, the centralisation of data within a state-controlled repository for Australia's COVIDSafe[22] app also drew speculation about potential data breaches since mass volumes of data are being stored only in a single government database.[23] 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.[24] 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.[25]

In Singapore, COVID data collected is not only sourced from the local contact tracing app, TraceTogether,[26] but also via state surveillance and monitoring technologies. This combination of data generators includes mandatory electronic wristbands issued to inbound travellers, which must be worn for the entire duration of their stay-home notice if they reside outside of quarantine facilities.[27] Such measures had been earlier introduced in Hong Kong, where all inbound overseas travellers were ordered to wear electronic bracelets (capable of identifying

[20] Gary Adshead, '"Unforgivable": The Privacy Breach That Exposed Sensitive Details of WA's Virus Fight' (*WAtoday*, 20 July 2020) <https://www.watoday.com.au/national/western-australia/unforgivable-the-privacy-breach-that-exposed-sensitive-details-of-wa-s-virus-fight-20200720-p55dsm.html> accessed 19 August 2020.

[21] Tiffany Fumiko Tai, 'Singaporeans Accept Some Privacy Loss in Covid-19 Battle but Surveillance Method Matters' (n 29).

[22] 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.

[23] 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.

[24] '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.

[25] '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.

[26] On 20 March 2020, TraceTogether was launched as part of ongoing tracing efforts to manage the COVID-19 outbreak in Singapore. See: 'Singapore Launches TraceTogether Mobile App to Boost COVID-19 Contact Tracing Efforts' (*CNA*) <https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616> accessed 7 August 2020.

[27] Tee Zhuo, 'Travellers to Singapore to Wear Electronic Tracking Device While Serving Covid-19 Stay-Home Notice Outside of Facilities' (*The Straits Times*, 3 August 2020) <https://www.straitstimes.com/singapore/covid-19-gps-tracking-device-for-travellers-to-singapore-on-stay-home-notice-outside-of> accessed 6 August 2020.

wearers even without their phones)[28] during home quarantine. The wearers of the technology receive reminders to take photographs of themselves together with the wristband.[29] Those who breached control regulations and stay-home notices faced a fine or imprisonment.[30]

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.[31] 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.[32] 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).[33]

Apps based on a consent approach require voluntary accession by the data subjects. Contact tracing apps, like COVIDSafe or TraceTogether, rely on the public's blanket trust and cooperation with the governing agency, based on a general, prevailing presumption that data will not be misused. However, Teo Yi-Ling, a senior fellow at the S. Rajaratnam School of International Studies' Centre of Excellence for National Security, highlighted that even though the Singapore government has stressed that measures have been taken to ensure that the collected data would not be misused, Singaporeans are still wary of past cyberattacks on government databases, particularly where personal health data is concerned. A significant cyberattack that generated massive public disquiet across Singapore occurred in June 2018, where hackers copied more than 1.5 million patients' hospital records, of which 160,000 entries recorded information about their

[28] Mary Meisenzahl, 'People Arriving in Hong Kong Must Wear Tracking Bracelets for 2 Weeks or Face Jail Time. Here's How They Work.' (*Business Insider*) <https://www.businessinsider.com/hong-kong-has-tracking-bracelets-to-enforce-coronavirus-quarantine-2020-4> accessed 6 August 2020.

[29] Meisenzahl (n 28).

[30] Tee Zhuo, 'Travellers to Singapore to Wear Electronic Tracking Device While Serving Covid-19 Stay-Home Notice Outside of Facilities' (n 106); Meisenzahl (n 107).

[31] Tiffany Fumiko Tai, *Singaporeans accept some privacy loss in Covid-19 battle but surveillance method matters: IPS study*, THE STRAITS TIMES (2020), https://www.straitstimes.com/singapore/singaporeans-accept-some-privacy-loss-in-covid-19-battle-but-surveillance-method-matters (last visited Jul 22, 2020).

[32] '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.

[33] Tiffany Fumiko Tai, 'Singaporeans Accept Some Privacy Loss in Covid-19 Battle but Surveillance Method Matters' (n 29).

outpatient dispensed medicines taken. This incident has been described by authorities as the "most serious breach of personal data".[34]

Varied technical standards and operational strategies for data-compilation have been scrutinised by Vice President of the European Commission, Margrethe Vestager, who noted that France's centralised approach to pandemic data collection (i.e. its central database which may be prone to cyberattack)[35] via StopCovid[36] is incompatible with the other EU member states that utilise the decentralised framework. This discrepancy also raises regional concerns, since the incongruity of France's app is a significant impediment in the EU's aims of unifying app developers across member states to potentially streamline data collection as people start to travel across the bloc.[37]

It is apparent that 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.

(b) Anonymity and re-identification and data privacy

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. In an example mentioned in the earlier subsection, 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.[38]

Similarly in South Korea, the wide harvesting and sharing of data (originally implemented during the outbreak of Middle East Respiratory Syndrome (MERS) in 2015)[39] amassed from credit card transactions, phone geolocation, surveillance footage, facial scans, and temperature monitors

[34] 'Why Aren't Singaporeans Using the TraceTogether App?' (*South China Morning Post*, 18 May 2020) <https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether> accessed 20 July 2020.

[35] 'France's COVID Tracing App Hard to Link to Others, EU Official Says' *Reuters* (16 June 2020) <https://www.reuters.com/article/us-health-coronavirus-app-france-idUSKBN23N2KL> accessed 19 August 2020.

[36] On 3 June 2020, France launched its digital tracing app, CovidStop. 'France Releases Contact-Tracing App StopCovid' (*TechCrunch*) <https://social.techcrunch.com/2020/06/02/france-releases-contact-tracing-app-stopcovid-on-android/> accessed 1 September 2020.

[37] 'France's COVID Tracing App Hard to Link to Others, EU Official Says' (n 35).

[38] Dr Vanessa Teague Melbourne Dr Chris Culnane and Dr Ben Rubinstein, University of, '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.

[39] '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.

were employed to enforce targeted lockdowns.[40] 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,[41] 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,[42] 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 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,[43] 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.[44]

[40] '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.

[41] '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.

[42] 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.

[43] '9 Geeky Myth-Busting Facts You Need to Know about TraceTogether' (n 32); 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.

[44] 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.

(c) Duration of retention of data

Despite calls for deletion of data after it has fulfilled its health protection purpose,[45] this has not prevented governments from justifying permanent retention,[46] as was the case in South Korea which sought to permanently retain health data after the MERS outbreak ended.[47]

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[48] applies to individuals and business organisations and not to the government.[49] 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.

(d) Nature of data

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.[50]

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

[45] 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.

[46] 'Privacy vs. Pandemic Control in South Korea' (n 39).

[47] '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.

[48] 'Personal Data Protection Act 2012 - Singapore Statutes Online' <https://sso.agc.gov.sg/Act/PDPA2012> accessed 13 October 2020.

[49] 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.

[50] 'How Governments Can Build Trust in AI While Fighting COVID-19' (n 40).

officials, rather than government officials at large. In addition, the same survey interestingly noted:[51]

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

2. Disquiet surrounding authority styles (external to the technologies employed)

(a) The adoption of intrusive control strategies and its manner of implementation

Most recently, the Singapore government has announced a pilot programme combining the use of SafeEntry and TraceTogether data to improve the contact tracing process.[52] SafeEntry, an island-wide mandated digital check-in system that logs data subjects' visited locations, relies on location records.[53] 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.[54] 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.[55] This conflation of technology

[51] 'Singaporean Attitudes to Personal COVID Data Differ to Overseas Counterparts' (15 April 2020) <https://www.consultancy.asia/news/3126/singaporean-attitudes-to-personal-covid-data-differ-to-overseas-counterparts> accessed 27 July 2020.

[52] 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.

[53] 'How Are My Possible Exposures Determined?' (*TraceTogether FAQs*) <http://support.tracetogether.gov.sg/hc/en-sg/articles/360053464873> accessed 10 September 2020.

[54] 'How Does the TraceTogether App Work?' (*TraceTogether FAQs*) <http://support.tracetogether.gov.sg/hc/en-sg/articles/360043543473> accessed 11 September 2020.

[55] '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;

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.[56] 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.[57] In addition, by making a 70% take-up rate of TraceTogether a condition for re-opening up the country,[58] this confirms the state's prioritization of more stringent surveillance rather than citizen self-determination.

Surveillance disproportionately affects data subjects across societies, depending on their situational vulnerability (such as residential status and occupational exposure) in terms of 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.[59] 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.[60] 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.[61]

'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.

[56] '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.

[57] 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.

[58] '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.

[59] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' (n 32).

[60] 'Attitudes towards the Use of Surveillance Technologies in the Fight against COVID-19' (n 32).

[61] 'How Governments Can Build Trust in AI While Fighting COVID-19' (n 40).

In Australia, intrusive control measures are not as widely accepted by data subjects compared to Singapore.[62] As such, to counter the slow uptake of contact tracing apps following inadequate clarifications and growing distrust, federal authorities mooted compulsory citizen subscription.[63] 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.[64] 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.[65] However, officials quickly back-peddled on mandatory downloads owing to public backlash against suggestions of political coercion.[66] In a tweet, Prime Minister Scott Morrison expressly stated that the app will "not be mandatory".[67] 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.[68] 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.[69]

[62] Within the Coalition government, parliamentarians have explicitly declared their resistance to downloading the COVIDSafe app amidst growing privacy and rights concerns. Alternatively Singapore's political arrangements, strong systems of social control, along with sanctioning of alternative voices and expressions of opposition has contributed to the relative lack of resistance by Singaporean data subjects. For more a more detailed discussion, see: Gerard Goggin, 'COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology' [2020] Media International Australia 1329878X20949770.

[63] '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.

[64] The legislation is detailed in 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.

[65] '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.

[66] '"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.

[67] '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.

[68] Reuters, 'Australia's Victoria State to Deploy Military, Impose A$5,000 Fines to Enforce Coronavirus Isolation' (n 54).

[69] '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.

In response, sections of the Australian public have sought to counter the government's control responses through nationwide protests (including Melbourne,[70] New South Wales,[71] and more specifically Sydney[72]) against lockdown measures. Hundreds of anti-lockdown protestors gathered together during "Freedom Day" rallies, chanting "freedom" and "human rights matter",[73] 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.[74]

In a similar vein, India has already directed that their tracing app, Aarogya Setu (launched in April 2020),[75] be downloaded by government employees and private sector workers,[76] as well as those living in containment zones. During the period of mandate, data subjects risked a potential jail term of up to 6 months for non-compliance.[77] The state's limited attempts at safeguarding privacy only aggravated the negative consequences of compulsion: especially during the app's launch, where users could not consent to whether personal data was being shared with law enforcement agencies and third parties (until the updates in July 2020), which could result in potential misuse, abuse and discrimination.[78]

[70] '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 Ashleigh McMillan, Rachael, '"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.

[71] '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.

[72] '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.

[73] 'Arrests Made at Anti-COVID-19 Protests in Sydney' (n 72); 'Coronavirus: Arrests at Australia Anti-Lockdown Protests' (n 70).

[74] 'Coronavirus: Arrests at Australia Anti-Lockdown Protests' (n 70).

[75] Launched on 2 April 2020, the central government mandated the use of Aarogya Setu for all workers. See 'Aarogya Setu App Hits 5 Crore Users in 13 Days of Launch' (*NDTV Gadgets 360*) <https://gadgets.ndtv.com/apps/news/aarogya-setu-app-total-users-downloads-5-crore-android-ios-2211990> accessed 1 September 2020; Andrew Clarance, 'Why Is India's Contact Tracing App Controversial?' *BBC News* (15 May 2020) <https://www.bbc.com/news/world-asia-india-52659520> accessed 5 August 2020.

[76] Legal experts have questioned the basis of such mandate, as this is not backed by any existing laws. Clarance (n 75). As a result, the government has issued guidelines removing the mandate: Neetu Chandra Sharma, 'Government Climbs down on Aarogya Setu by Removing Mandatory Provision' (*Livemint*, 30 May 2020) <https://www.livemint.com/news/india/government-climbs-down-on-aarogya-setu-by-removing-mandatory-provision-11590850319300.html> accessed 5 August 2020.

[77] Clarance (n 75).

[78] Priyali Sur Business CNN, 'Many Indian Citizens Believe Their Government Is Trying to Steal and Sell Their Data. Here's Why' (*CNN*) <https://www.cnn.com/2020/06/21/tech/india-privacy-app-hnk-intl/index.html> accessed 5 August 2020; 'Aarogya Setu and Patient Tracking Tools: A Serious Infringement of Digital Privacy | The Indian Express' <https://indianexpress.com/article/opinion/aarogya-setu-patient-tracking-tool-data-privacy6431644/> accessed 5 August 2020; 'Aarogya Setu: Who Can Access Your Data, and When?' (*The Indian Express*, 14 May 2020) <https://indianexpress.com/article/explained/coronavirus-aarogya-setu-who-all-can-access-your-data-and-when-6407175/> accessed 5 August 2020.

(b) Information deficit, lack of transparency and explainability

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".[79] 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.

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),[80] 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.[81]

In Southeast Asia, Indonesia's PeduliLindungi[82] 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.[83] 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.

[79] Reference made to the tables in the Appendix.

[80] Australian Government Department of 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.

[81] Greenleaf and Kemp (n 64).

[82] 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.

[83] '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.

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.[84] Similarly, 18 organisations wrote an open letter to the Philippines' government, making analogous requests for strong user protections over its StaySafe.ph's app.[85]

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.[86] 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.

(c) Accountability of authorities

Data subject frustrations also stem from misleading statements made by the government regarding the operations of tracking/tracing apps. For example, an interview with the Australian Minister for Government Services, Stuart Robert, noted that the defined proximity used for the app was 1.5 meters for 15 minutes.[87] The government also stated data collected from phones were limited to those within the defined proximity.[88] While the aforementioned statements were later discovered to be untrue, no steps appear to have been taken by officials to clarify such misstatements with the public, further aggravating distrust about accountability and transparency assertions.[89] The incorrect or incoherent dissemination of information to the community not only erodes public confidence necessary to encourage app downloads, but also sows wider distrust in the government's management of the crisis.[90]

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 as

[84] 'Open Letter to KOMINFO Requesting for Strong User Privacy Protections in the PeduliLindungi App' (*DigitalReach*, 30 June 2020) <https://digitalreach.asia/open-letter-to-kominfo-requesting-for-strong-user-privacy-protections-in-the-pedulilindungi-app/> accessed 5 August 2020.

[85] '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.

[86] Findlay, Milne and Palma (n 44).

[87] 'Interview with Natalie Barr, Sunrise' (17 April 2020) <https://minister.servicesaustralia.gov.au/transcripts/2020-04-17-interview-natalie-barr-sunrise> accessed 4 August 2020.

[88] Max Koslowski, 'Coronavirus Tracking App: How Will the COVID-19 Contact Tracing App Work?' (*The Sydney Morning Herald*, 4 May 2020) <https://www.smh.com.au/politics/federal/how-will-the-coronavirus-app-work-20200421-p54ltg.html> accessed 4 August 2020.

[89] Greenleaf and Kemp (n 64).

[90] Greenleaf and Kemp (n 64).

developers encountered Bluetooth performance obstacles.[91] 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.[92] When queried again on 5 June 2020, Minister Nadhim Zahawi admitted that he could not give an exact release date for the app.[93] 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.[94] 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.[95] The chaotic mismanagement of the contact tracing app has been labelled as a debacle,[96] with many demanding an explanation as to why publicly aired enquiries remain unaddressed and dismissed.[97]

(d) Reframing consent into a moral imperative

Another strategy adopted by governments to increase participation in state-sponsored contact tracing initiatives is through promoting the rhetoric of citizenship and its associated duties to garner support for the use of the technology. In the United Kingdom, Health Secretary Matt Hancock proposed that citizens fulfilled their 'civic duty' by using any trace and track app.[98] Similarly in Australia, Prime Minister Morrison stated that citizens ought to download the COVIDSafe app "as a matter of national service."[99] A similar rhetoric is used in Singapore, with the government declaring that there must be a collective uptake of TraceTogether by at least 70% of phone users before further steps can be taken to re-open the country.[100] Commentators

[91] Leo Kelion, 'Ministers Consider Coronavirus-Tracing App Rethink' *BBC News* (11 June 2020) <https://www.bbc.com/news/technology-52995881> accessed 3 August 2020.

[92] 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.

[93] '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.

[94] 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.

[95] 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.

[96] '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.

[97] 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; 'The UK's Contact Tracing App Fiasco Is a Master Class in Mismanagement' (n 96).

[98] Boseley and Stewart (n 13); 'Matt Hancock Says Public Has a "duty" to Download Coronavirus Contact Tracing App' (n 13).

[99] 'Australians Urged to Adopt Phone Tracking App in Coronavirus Fight' *Reuters* (17 April 2020) <https://uk.reuters.com/article/uk-health-coronavirus-australia-idUKKBN21Z03M> accessed 20 August 2020.

[100] 'TraceTogether SafeEntry Token & App Must Be Used by 70% of S'pore Population to Enter Phase 3' (n 58).

have suggested that the reliance on such deontological narratives to promote compliance detracts from the voluntary premise of using tracing apps. Instead, citizens are pressured to engage in enhanced surveillance measures not voluntarily but fearing that negative inferences about their 'good citizenship' could be drawn from choosing to opt out (a choice it might be argued which is inherent in the freedoms of self-determination).[101]

(e) Availability of legal recourses and mechanisms

Faced with risks of privacy infringements and data breaches, it should be remembered that data subjects do not always possess suitable remedies. For instance, Australians do not have strong personal legal recourse to challenge privacy infringements by the state, considering that fundamental privacy rights are not accorded by Australia's constitution, treaty obligations, or even common law. [102] Even so, the Privacy Protection Act (1988) provides circumscribed protections against the misuse of personal data by government agencies and major private sector entities. Legal mechanisms to safeguard the use and retention of data collected, not grounded in unambiguous rights of privacy, may not prove sufficient to combat or deter potential misuse like the prolonged retention of app data beyond its prescribed promised period. Interestingly, in the Australian context, the Australian Law Reform Commission is presently directing its recommendations on citizens' rights in situations of technological advancement, using a human rights discourse, and proposing legal recourse for breach.

However, even constitutional rights of privacy may not provide a fool-proof answer to data abuse in emergency settings. In South Korea, the use of aggressive testing and large-scale intrusive surveillance technologies on its citizens[103] has drawn criticism given that the disproportionate disclosure of personal location information has been recognised as a violation of basic human rights and personal privacy.[104] In theory, unlike Australian citizens, Koreans have recourse to a comprehensive data protection and privacy regime under the Personal Information Protection Act and enforcement regulations,[105] which requires data to be deleted after it has been used for its intended purpose. However, more exhaustive legislation does not appear to adequately protect the rights to privacy of individual in every instance of breach. As mentioned previously, the Korean government recently admitted to permanently retaining patients' data from its earlier

[101] 'COVID-19: How Public Health Emergencies Have Been Repurposed as Security Threats' <https://www.adalovelaceinstitute.org/covid-19-how-public-health-emergencies-have-been-repurposed-as-security-threats/> accessed 17 August 2020.

[102] 'Australia, Right to Privacy' <http://www.hrcr.org/safrica/privacy/austr_law.html#:~:text=There%20is%20no%20general%20legal,privacy%20in%20Anglo%2DAustralian%20law.&text=This%20is%20done%20by%20establishing,to%20Commonwealth%20departments%20and%20agencies.> accessed 4 August 2020; Greenleaf and Kemp (n 64).

[103] 'How Governments Can Build Trust in AI While Fighting COVID-19' (n 40).

[104] The Petrie-Flom Center Staff, 'COVID-19 in South Korea: Privacy and Discrimination Concerns' (*Bill of Health*, 9 June 2020) <http://blog.petrieflom.law.harvard.edu/2020/06/09/south-korea-global-responses-covid19/> accessed 5 August 2020.

[105] 'Personal Data Protection Laws in Korea' <https://www.privacy.go.kr/eng/laws_view.do?nttId=8186&imgNo=4> accessed 5 August 2020.

epidemics.[106] Despite stringent privacy protection laws, the government's downplaying of privacy safeguards allowed data leaks and unwarranted surveillance on individuals to persist.

3. Disquiet surrounding the internal architecture of control technologies employed (inherent to the devices)

(a) Overselling and overpromising the privacy-protection capacities of technologies

Technology sponsors have repeatedly made unsubstantiated or unreasonable guarantees regarding the privacy protections inherent in their applications, particularly those operating via Bluetooth connectivity.[107] 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,[108] and contact tracing apps like Norway's Smittestopp[109] 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 public who then later criticised this practice as being too invasive of privacy, upon discovery.[110] 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.[111]

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 supressed 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

[106] 'South Korea Admits Keeping Personal Data Of 2015 MERS Outbreak Patients' (n 47).

[107] 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.

[108] '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.

[109] 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.

[110] '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.

[111] Goggin (n 62).

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.[112] As a response to privacy concerns, Apple and Google's partnership in the creation of the Exposure Notification System[113] utilises a "decentralised" approach which is commended for data collection without a centralised database,[114] thereby effectively limiting the consequences that arise from data breaches in a single large repository.

(b) Effectiveness and functionality of technologies

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.[115] 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 alerted to such a problem,[116] leaving many to question the accuracy of such surveillance and the genuine utility of their related apps.[117]

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.[118] 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

[112] Sharon (n 23).

[113] 'Privacy-Preserving Contact Tracing - Apple and Google' (*Apple*) <https://www.apple.com/covid19/contacttracing> accessed 30 July 2020.

[114] 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; Kelion (n 95).

[115] 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.

[116] '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.

[117] 'China's Coronavirus Health Code Apps Raise Concerns over Privacy' (n 116).

[118] Cellan-Jones (n 92).

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.[119] Despite the appeal of such apps, initial research has suggested that these technologies (centralised or decentralised) have not significantly aided the contact tracing process.[120]

Singapore's new self-check system[121] will potentially see a growth of false positive numbers as is already evident in exposure notification apps,[122] 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.[123]

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)[124] 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.[125] 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 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

[119] '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.

[120] 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.

[121] 'Strengthening Measures for Safe Reopening of Activities' <http://www.gov.sg/article/strengthening-measures-for-safe-reopening-of-activities> accessed 10 September 2020.

[122] 'The Importance of Equity in Contact Tracing' (*Lawfare*, 1 May 2020) <https://www.lawfareblog.com/importance-equity-contact-tracing> accessed 24 September 2020.

[123] Mark Findlay and others, 'Strengthening Measures for Safe Reopening of Activities: Ethical Ramifications and Governance Challenges'.

[124] 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.

[125] 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.

of much more intrusive control responses like the imposition of a state-wide militarised curfew.[126]

(c) Understandability and explainability of technologies

Much community unease surrounds the surveillance technology itself, considering that the common user or data subject does not possess the necessary technical understanding of the workings behind apps or appreciate facial recognition software functions.[127] To its credit, the Singaporean authorities have sought to bridge the gap in technical knowledge on the operability of COVID technologies. A brief examination of the Singapore authorities' responses to data subjects' experiences with TraceTogether demonstrates the efforts made to increase understandability of the contact tracing app, along with their shortfalls.

Users typically download contact tracing apps from Google's Play Store and Apple's App store and are encouraged to review apps on the platforms from which they download. This has become an interesting source of disquiet expressed in user reviews. The Appendix details several instances of user frustrations and confusions regarding the interactions of Singapore's TraceTogether app. At the time of writing, the TraceTogether app has received a 4.0 star rating (derived from over 7,377 reviewers)[128] on the Google Play Store, and a 3.8 star rating (from over 239 reviewers) on the Apple Apps Store.[129] The limited reviews and lack of take up from Apple users may be largely attributable to the fact that since its launch on the app store on 20 March 2020,[130] TraceTogether could only run in the foreground in iPhones (meaning that users had to constantly reopen the TraceTogether app on their phone after using another app). In this configuration, TraceTogether could not run in background as was originally intended and this led to excessive battery drain prior to its update in July (which has since resolved a majority of the technological issues).[131] With frustrating technical shortcomings and user interface disruptions,

[126] Reuters, 'Australia's Victoria State to Deploy Military, Impose A$5,000 Fines to Enforce Coronavirus Isolation' (n 48).

[127] 'Scattergun Procurement Exposes NHSX to Question of Fitness' (*Healthcare IT News*, 28 May 2020) <https://www.healthcareitnews.com/news/europe/scattergun-procurement-exposes-nhsx-question-fitness> accessed 30 July 2020; 'NHSX "Knew Contact-Tracing App Wouldn't Work on IPhones in April"' (*Digital Health*, 24 June 2020) <https://www.digitalhealth.net/2020/06/nhsx-knew-contact-tracing-app-wouldnt-work-on-iphones-in-april/> accessed 30 July 2020; Ryan Browne, 'Why Coronavirus Contact-Tracing Apps Aren't yet the "game Changer" Authorities Hoped They'd Be' (*CNBC*, 3 July 2020) <https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html> accessed 30 July 2020.

[128] 'TraceTogether – Apps on Google Play' <https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace&hl=en_SG> accessed 7 August 2020.

[129] 'TraceTogether' (*App Store*) <https://apps.apple.com/sg/app/tracetogether/id1498276074> accessed 7 August 2020.

[130] 'Singapore Launches TraceTogether Mobile App to Boost COVID-19 Contact Tracing Efforts' (n 26).

[131] 'Coronavirus: Contact Tracing App Update Fixes Battery Drain in IPhones' (*The Straits Times*, 7 July 2020) <https://www.straitstimes.com/singapore/contact-tracing-app-update-fixes-battery-drain-in-iphones> accessed 7 August 2020.

many Apple operators were unwilling to use TraceTogether, thereby limiting the digital contact tracing efforts.[132]

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.[133] 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", [134] 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.[135]

As a result, if the basic user's only interaction with the government body responsible for developing the app is largely restricted to the replies received in the Play Store or App Store to questions raised, there may be an unbalanced perception that the government body is making insufficient efforts to explain the utility of tracing apps, or does not feel the need to account to data subjects on how the app is used and its statistics determined. Therefore, information deficit

[132] 'Given Low Adoption Rate of TraceTogether, Experts Suggest Merging with SafeEntry or Other Apps' (*TODAYonline*) <https://www.todayonline.com/singapore/given-low-adoption-rate-tracetogether-experts-suggest-merging-safeentry-or-other-apps> accessed 7 August 2020.

[133] Jason Bay and others, 'BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing across Borders' 9; Goggin (n 62).

[134] '9 Geeky Myth-Busting Facts You Need to Know about TraceTogether' (n 43).

[135] 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.

negatively influences the efficacy of the app. Without appropriate and easily accessible explanations and clarifications supporting it, people currently using the app, or wishing to use the app, may remain reluctant to participate in contact tracing via TraceTogether due to lingering misconceptions.

4. Disquiet surrounding the infringement of rights and liberties

(a) Discriminatory practices

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.[136] 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.

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.[137] 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 in their communities at many levels and with varying degrees of intrusion.[138] Law enforcement secondary surveillance purposes complement patterns of selective policing, wherein certain minorities and targeted communities are overpoliced in any event.[139]

[136] 'Should I Worry about Mass Surveillance Due to COVID-19?' (n 110).

[137] '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.

[138] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).

[139] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).

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"[140] 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.[141]

As alluded to above,[142] 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.[143] 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.[144]

Nevertheless, 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".[145] 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.[146] However, whether or not states translate this awareness into firm policy qualifiers for reducing emergency surveillance measures remains to be seen.

In attempts to enforce lockdowns, there are reports regarding disproportionate targeting of ethnic minorities and marginalised groups with violence, unwarranted and unnecessary identity

[140] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[141] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).
[142] 'Privacy Is Not the Problem with the Apple-Google Contact-Tracing Toolkit | Michael Veale' (n 137).
[143] '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.
[144] 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; The Korea Herald, 'Korean Media's Focus on "Gay" Club in COVID-19 Case Further Stigmatizes LGBT People' (8 May 2020) <http://www.koreaherald.com/view.php?ud=20200508000751> accessed 6 August 2020; 'South Korea's Coronavirus Contact Tracing Puts LGBTQ Community under Surveillance, Critics Say' (n 143).
[145] '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.
[146] 'Cyber-Intel Firms Pitch Governments on Spy Tools to Trace Coronavirus' (n 145).

checks, especially in poorer areas of cities.[147] 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.[148] 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[149] recorded that the number of fines issued during lockdown for violating regulations tripled the rest of the nation, despite assurances from authorities that lockdown measures were uniform throughout the country.[150]

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.[151]

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.[152] 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"?[153]

[147] '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.

[148] 'COVID-19_and_Racial_Discrimination.Pdf' <https://www.ohchr.org/Documents/Issues/Racism/COVID-19_and_Racial_Discrimination.pdf> accessed 6 August 2020.

[149] '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.

[150] '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.

[151] 'COVID-Tech: Surveillance Is a Pre-Existing Condition' (n 14).

[152] 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.

[153] The Associated Press (n 152).

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.[154] 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.[155]

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.

(b) Privacy Rights

Privacy is understood differently across various social, political, cultural and economic contexts, as evidenced by the different levels of support for, or distrust of, data collection initiatives by public and private agencies in specific social situations. While many data subjects are prepared to tolerate short-term privacy invasions in exchange for the possibility of returning to a pre-COVID-19 normalcy, the acceptance and the increasing regularization of surveillance technology (whether such technology (and its data) are controlled by public authorities or private corporations) is alarming critical commentators,[156] and has produced debates and concerns about whether rights to freedom and privacy are being more permanently curtailed, or simply downplayed through COVID fatigue.[157] The correlation between pre-pandemic public surveillance, strong state authority, and community compliance is not surprising.[158] In other communities and jurisdictions which are less accustomed to the surveillance state, less intrusive technology has been met with disquiet and even active resistance.

[154] 'Policing the Pandemic - Human Rights Violations in the Enforcement of COVID-19 Measures in Europe.' (n 149).

[155] '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.

[156] '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.

[157] 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.

[158] 'Would You Risk Your Privacy to Relax Lockdown Sooner?' (*The Independent*, 8 May 2020) <https://www.independent.co.uk/news/long_reads/coronavirus-lockdown-korea-singapore-turkey-surveillance-privacy-tracking-app-a9499526.html> accessed 4 August 2020.

The use of multimodal surveillance technologies combined with such abovementioned data breaches have resulted in repeated, large-scale invasions privacy for data subjects. Reactions to these common violations of rights and dignity are not consistent, due in part to different appreciations of the value of rights under threat, and the compromise through a return to regular socialising.

In the United Kingdom, calls have been made by medical professionals for an assessment of contact tracing apps after the United Kingdom's Department of health admitted that their test and trace programme had violated the EU's General Data Protection Regulation (GDPR).[159] The surveillance strategy was deemed to be unlawful given the lack of adequate assessments of its privacy implications prior to its intended launch.[160] A UK-based digital rights organisation, the Open Rights Group, cautioned that the government's disregard of basic privacy safeguards in its test and trace app may lead to the erosion of mutual trust between the public and the state, which has been a recurrent theme throughout this paper.[161]

The EU control efforts also reveal disparate attitudes towards privacy concerns. In France, the StopCovid app was rolled out amid privacy controversies, as civil liberties groups worried that app was a gateway for government surveillance since the limited utilisation of health data collected was unclear.[162] Just two weeks after its launch, cryptography researcher Gaëtan Leurent discovered that the app had initially collected more data than necessary (or originally promised to citizens) and were being uploaded to the central server, in violation of the data minimisation principle.[163] The public was originally informed that only contacts who were in the proximity of 1 metre for at least 15 minutes would be collected and sent to storage.[164] However, it appeared that even passing and far away contact information was being collated and disseminated to the central server.[165] In addition, the European Commission had observed that

[159] Rory Cellan-Jones, 'England's Test and Trace Scheme "Breaks Data Law"' *BBC News* (20 July 2020) <https://www.bbc.com/news/technology-53466471> accessed 5 August 2020.
[160] Cellan-Jones (n 159).
[161] Naomi Owen, 'England's Test and Trace App Could Face Lawsuit for Breaching GDPR' (*PrivSec Report*, 21 July 2020) <https://gdpr.report/news/2020/07/21/englands-test-and-trace-app-could-face-lawsuit-for-breaching-gdpr/> accessed 5 August 2020.
[162] Associated Press, 'French Virus Tracing App Goes Live amid Debate over Privacy' (*Los Angeles Times*, 2 June 2020) <https://www.latimes.com/world-nation/story/2020-06-02/french-coronavirus-tracing-app-goes-live-debate-privacy> accessed 5 August 2020.
[163] 'Gaëtan Leurent on Twitter: "I Just Realized That #StopCovid Seems to Send All Contacts to the Server, Even Passing on the Other Side of the Street. This Would Contradict the Official Decree (Contacts of 15min at 1m), and Violate Data Minimization Principle Required by @CNIL and #GDPR Https://T.Co/TV7yj0AuSZ" / Twitter' (*Twitter*) <https://twitter.com/cryptosaurus6/status/1271500543349764096> accessed 5 August 2020; 'Art. 5 GDPR – Principles Relating to Processing of Personal Data' (*General Data Protection Regulation (GDPR)*) <https://gdpr-info.eu/art-5-gdpr/> accessed 5 August 2020.
[164] 'Info Coronavirus COVID-19 - STOPCOVID' (*Gouvernement.fr*) <https://www.gouvernement.fr/info-coronavirus/stopcovid> accessed 5 August 2020.
[165] 'Gaëtan Leurent on Twitter: "I Just Realized That #StopCovid Seems to Send All Contacts to the Server, Even Passing on the Other Side of the Street. This Would Contradict the Official Decree (Contacts of 15min at 1m), and Violate Data Minimization Principle Required by @CNIL and #GDPR Https://T.Co/TV7yj0AuSZ" / Twitter' (n 163). As of 28 June 2020, Gaëtan Leurent tweeted an update on this matter, stating that the latest version of StopCovid

the French app was incompatible with other apps used in the EU given the different data storing methods.[166]

On the other hand, privacy commentaries that condemned the French technology have not been apparent in Germany as its app, Corona-Warn-App, [167] has won much praise for its transparency.[168] 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.[169] Data is both collected and encrypted,[170] 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 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.[171]

Taking a hybrid approach, Italy's contact tracing app, Immuni,[172] 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.[173]

appears to discard short term and far away contacts: 'Gaëtan Leurent on Twitter: "Good News, the Latest Version of #StopCovid Apparently Discards Short Contacts, and Far Away Contacts. That's Clearly an Improvement, but More Communication Would Be Nice (There Is No Official Answer on the GitLab)." / Twitter' (*Twitter*) <https://twitter.com/cryptosaurus6/status/1277230052044943362> accessed 5 August 2020.

[166] 'French App StopCovid Still Facing Hurdles amid EU Concerns about Data Access' (*RFI*, 17 June 2020) <https://www.rfi.fr/en/science-and-technology/20200617-french-tracing-mobile-phone-app-stopcovid-meets-first-stumbling-blocks-fails-to-convince-coronavirus-health-privacy-science-technology> accessed 5 August 2020.

[167] 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.

[168] 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.

[169] '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.

[170] 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.

[171] 'Internetauftritt Des Bundesbeauftragten Für Den Datenschutz Und Die Informationsfreiheit - Press Office - Sufficient Data Protection in the Corona Warning App' (n 169).

[172] 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.

[173] Hadas Gold Business CNN, '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.

(c) *Potential restrictions on free speech*

Experts have observed that the pandemic may be argued to be a catalyst for further expansion of surveillance regimes, especially in countries that do not have stringent laws governing personal data protection.[174] In addition, the overreaching of heightened surveillance powers would enable governments to further invade privacy, deter free speech, and disparately discriminate against vulnerable groups in the community.[175] As Michael Abramowitz, president of Freedom House (a US government-funded non-governmental organisation) observed, there have been "signs that authoritarian regimes are using COVID-19 as a pretext to suppress independent speech, increase surveillance, and otherwise restrict fundamental rights, going beyond what is justified by public health needs".[176]

5. Disquiet surrounding the role of the private sector

(a) *Concentration of power in the hands of technological giants*

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 technological companies encroaching into territories of political and medical policy. In Dr Tamar Sharon's view: [177]

> 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".[178] The ability of tech giants like Apple and Google to

[174] '"The New Normal": China's Excessive Coronavirus Public Monitoring Could Be Here to Stay' (*the Guardian*, 9 March 2020) <http://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay> accessed 20 July 2020.

[175] Bangkok Post Public Company Limited, 'Privacy Rights May Become next Victim of Killer Pandemic' (*https://www.bangkokpost.com*) <https://www.bangkokpost.com/world/1888705/privacy-rights-may-become-next-victim-of-killer-pandemic> accessed 20 July 2020.

[176] 'Freedom House - Home' <https://www.facebook.com/FreedomHouseDC/> accessed 22 July 2020.

[177] Sharon (n 23).

[178] Sharon (n 23).

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.[179] 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.[180]

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.[181] 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 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.[182]

[179] Sharon (n 23).

[180] Sharon (n 23).

[181] 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.

[182] '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.

(b) Values and interests of non-specialised private actors

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. [183]

6. Uncertainties surrounding the post-pandemic world and "the new normal"

(a) Justification for greater surveillance in the future

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,[184] and thermal scanners now display commuters' infrared images in train stations.[185] 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.[186] 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.[187] 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.[188]

[183] Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (Columbia Global Reports 2018).
[184] 'Coronavirus Brings China's Surveillance State out of the Shadows' (n 11).
[185] Stephen R, '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.
[186] 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.
[187] CNN (n 42).
[188] CNN (n 42).

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).[189]

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.[190]

(b) Retention of mass surveillance post-pandemic

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.[191] Presently, states justify the need for biometric surveillance in order to prevent further waves of virus or a new strains of infectious disease.[192] That said, state agencies may maintain the heightened levels of surveillance post-pandemic rather than reckoning with difficulties in scaling down their activities.[193] 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.[194] In this respect, community disaffection and pressure for inclusion and monitoring provides important checks and balances over a surveillance society future.

[189] Motsenok and others (n 10).
[190] Findlay and Remolina (n 15).
[191] 'Should I Worry about Mass Surveillance Due to COVID-19?' (n 110).
[192] Wim Naudé, 'Artificial Intelligence vs COVID-19: Limitations, Constraints and Pitfalls' [2020] Ai & Society 1.
[193] Kharpal (n 16).
[194] 'How to Protect Both Public Health and Privacy' (n 156).

(c) Utility of implementing sunset clauses

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.[195] 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.

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, Montsenok 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.[196]

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.[197] 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.

[195] Sharon (n 23).

[196] Motsenok and others (n 10).

[197] '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.

Section 3: Sources of Disquiet

Disquiet surrounding:		Source of Disquiet	Medium
Data Collected	Safety, integrity, security, and storage of personal data	Data subjects and the public	News articles, social media
		Experts/Commentators/Researchers	Journal articles
	Anonymity and re-identification and data privacy	Data subjects and the public	News articles
		Experts/Commentators/Researchers	Journal articles
	Duration of retention of data	Experts/Commentators/Researchers	Journal articles
	Nature of Data	Data subjects and the public	News articles, social media
Authority styles (external to technologies employed)	The adoption of intrusive control strategies and its manner of implementation	Data subjects and the public	News articles
		Workers in Employment	Survey
		Experts/Commentators/Researchers	Journal articles
		Advocacy groups/Civil liberty groups/Non-governmental organizations	Open letters, news articles, blogposts, social media
	Information deficit, lack of transparency and explainability	Data subjects and the public	News articles, social media
		Advocacy groups/Civil liberty groups/Non-governmental organizations	Open letters, news articles, blogposts, social media
	Accountability of authorities	Data subjects and the public	News articles
		Experts/Commentators/Researchers	Journal articles

Disquiet surrounding:		Source of Disquiet	Medium
	Reframing consent into a moral imperative	Experts/Commentators/Researchers	Journal articles
	Availability of legal recourses and mechanisms	Advocacy groups/Civil liberty groups/Non-governmental organizations	Open letters, news articles, blogposts, social media
Internal architecture of control technologies employed (inherent to the devices)	Overselling and overpromising the privacy-protection capacities of technologies	Experts/Commentators/Researchers	Journal articles, news articles
	Effectiveness and functionality of technologies	Data subjects and the public	News articles, social media
		Advocacy groups/Civil liberty groups/Non-governmental organizations	Open letters, news articles, blogposts, social media
		Government authorities	News articles, news briefings
	Understandability and explainability of technologies	Data subjects and the public	User reviews/ social media
Infringement of rights and liberties	Discriminatory practices	Advocacy groups/Civil liberty groups	Open letters, news articles, blogposts, social media
	Privacy Rights	Data subjects and the public	News articles, social media
		Advocacy groups/Civil liberty groups/Non-governmental organizations	Open letters, news articles, blogposts, social media
	Potential restrictions on free speech	Advocacy groups/Civil liberty groups	Open letters, news articles, blogposts, social media

Disquiet surrounding:		Source of Disquiet	Medium
Role of the private sector	Concentration of power in the hands of technological giants	Experts/Commentators/Researchers	Journal articles
	Values and interests of non-specialised private sectors	Experts/Commentators/Researchers	Journal articles
The post-pandemic world and the “new normal”	Justification for future surveillance in the future	Experts/Commentators/Researchers	Journal articles
	Retention of mass surveillance post-pandemic	Experts/Commentators/Researchers	Journal articles
	Utility of implementing sunset clauses	Experts/Commentators/Researchers	Journal articles

Section 4: Distrust and its effect on surveillance technology's utility and accuracy

1. The connection between distrust and failed utility

Throughout the above sections, 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[198] enabling citizens to check-in and out of venues,[199] 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.[200] 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.[201] 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.

[198] 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.

[199] '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.

[200] 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 56).

[201] 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.

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".[202] 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.[203] However, poor app reviews[204] and surging numbers of infections,[205] suggest that data subjects remain unsure about digital tracing technologies which could have a positive impact in hindering the spread of the virus.

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.[206] 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.

[202] 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.

[203] '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.

[204] 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.

[205] '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.

[206] 'Over 21,000 Signatures on Petition against Use of S'pore Govt-Issued Wearable Contact Tracing Devices' 00 <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.

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.

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”.[207] 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.[208]

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.

2. Managing confidence and ensuring that trust is not withdrawn

In countries where data subjects are willing to engage with control technology, governments should be vigilant not to abuse this trust and make efforts to ensure that public confidence is maintained. Uncertainties surrounding the duration of COVID-19 and the need to prevail with surveillance control technologies into an uncertain future have already resulted in public fatigue regarding the pressing necessity for pandemic control. Following on from any reduced sense of urgency and growing levels of resistance among some in the community, trust may be withdrawn at a greater rate from authorities arguing that containment of liberty and challenges to personal

[207] Harari (n 157).

[208] Harari (n 157).

data are outweighed by obvious increases in public safety.[209] Although data subjects initially displayed a willingness to participate in control efforts, the prolonged operation of tracing apps and the diversification of technological surveillance into other areas of community life will heighten citizen frustrations with the intrusive consequences of pandemic responses. The inconveniences felt daily by users who are eager to return to a pre-surveillance state of living are running against consensual compliance, and therefore the operational justifications of the apps are less persuasive as a counterbalance. The message that intrusion is the necessary cost of effective prevention and control may be losing its purchase, and distrust is a retarding social consequence as the efficacy of technological interventions is questioned.

The examples cited below demonstrate how data subjects' trust hangs on a very thin and fragile thread, and the lack of trust and confidence that will invariably result in the potential frustration of digital tracing efforts.

In Singapore, a user only has ability to consent to the use and retention of their data in the TraceTogether app until they are infected by the virus. Even though TraceTogether works on a by-consent approach, users who have tested positive for COVID-19 are compelled by law[210] to cooperate with health authorities by sharing data logs. Refusal is an offence under the Infectious Disease Act.[211] While this is arguably a moral or ethical obligation on the part of the data subject to share his information (so as to facilitate tracing efforts),[212] such a legal duty imposed only on infected data subjects calls into question notions that participation and data sharing rests on data subjects' consent. Despite the limited data that will be shared with the government by this reduced data subject population, it is uncertain whether potential criminalisation for withholding consent will deter the public participating in tracing technologies more generally.

In Germany, a widespread perception and recognition that the Corona-Warn-App is the 'best' tracing app by comparison with others in operation[213] has contributed to more than 15 million users signing up.[214] However, user confidence in the app was shaken by reports that the app had not been working for up to five weeks due to a technical issue that affected millions of Android

[209] Timothy Goh, '44% of People in Singapore Tired of Rules to Limit Covid-19 Spread: Survey' (*The Straits Times*, 16 August 2020) <https://www.straitstimes.com/singapore/health/44-of-people-here-tired-of-rules-to-limit-virus-spread-survey> accessed 2 September 2020.

[210] David Leslie, 'Tackling COVID-19 through Responsible AI Innovation: Five Steps in the Right Direction' [2020] SSRN Electronic Journal <https://www.ssrn.com/abstract=3652970> accessed 4 August 2020.

[211] Irene Tham, 'AskST: How New Token and App Will Address Privacy Concerns' (*The Straits Times*, 9 June 2020) <https://www.straitstimes.com/singapore/askst-how-new-token-and-app-will-address-privacy-concerns> accessed 14 August 2020.

[212] Owen Schaefer and Angela Ballantyne, 'Downloading COVID-19 Contact Tracing Apps Is a Moral Obligation' (*Journal of Medical Ethics blog*, 4 May 2020) <https://blogs.bmj.com/medical-ethics/2020/05/04/downloading-covid-19-contact-tracing-apps-is-a-moral-obligation/> accessed 1 October 2020.

[213] Deutsche Welle (www.dw.com), 'Germany Launches "best" Coronavirus Tracing App | DW | 16.06.2020' (*DW.COM*) <https://www.dw.com/en/germany-launches-best-coronavirus-tracing-app/a-53825213> accessed 2 September 2020.

[214] Christina Farr, 'Germany's Coronavirus Response Is a Master Class in Science Communication' (*CNBC*, 21 July 2020) <https://www.cnbc.com/2020/07/21/germanys-coronavirus-response-masterful-science-communication.html> accessed 2 September 2020.

and Apple users.[215] Apart from individual experiences with the app, news articles like Bloomberg's "Germany's Coronavirus Tracing App Won't Work"[216] and condemnatory opinions from dissenting politicians (i.e. Jens Zimmermann's criticism of the health authorities' lack of transparency or open communication) have compounded fears and frustrations that tarnish the earlier positive image, and aggravates a sense of distrust amongst data users. This evolving experience is evidence that public authorities and app developers need to prioritise user and data subject trust, in order to maintain the efficacy and utility of digital tracing efforts.

[215] Deutsche Welle (www.dw.com), 'Germany's Coronavirus Tracing App Criticized over Warning Failures | DW | 25.07.2020' (*DW.COM*) <https://www.dw.com/en/germanys-coronavirus-tracing-app-criticized-over-warning-failures/a-54305099> accessed 2 September 2020.

[216] 'Germany's Coronavirus Tracing App Won't Work' *Bloomberg.com* (16 June 2020) <https://www.bloomberg.com/opinion/articles/2020-06-16/germany-s-corona-app-is-much-worse-than-singapore-s> accessed 2 September 2020.

Section 5: The importance of citizen inclusion on app utility and effectiveness of control technology

The abovementioned themes of disquiet collectively reinforce the fact that data subjects perceive a lack of sufficient transparency surrounding both the surveillance technology and connected governmental strategies towards combating the virus. What follows is a collective sense of citizen disengagement and exclusion. Data subjects, whose personal information (mundane or health related) is being collected and whose participation that the government and app developers rely on for the effectiveness of this surveillance, significantly do not believe that they are being well informed, or have provided sufficient opportunity for input/feedback into the technology.

Citizen inclusion takes various forms – from contributing to drafting legislation to actively collaborating with civic-minded hackers and coders.[217] Indeed, those who are most directly impacted by the technologies are best-placed to assess its usability and efficacy.[218] Haines and Stevens have called for the need to revise public education to inform citizens about digital technology and privacy, and their implications on society and politics at large.[219]

In this section, we examine the importance of citizen inclusion and its utility in resolving pandemic-specific problems. We also emphasise the importance of healthy co-operation between public authorities and data subjects that facilitate control responses. Such cooperation from state actors and the private sector is both formal and informal, actual and virtual, and is ultimately inclusive and accountable.

1. Australia's legislative approach to COVID protection

The Australian government has admitted that to generate community trust and stimulate the effectiveness of its pandemic surveillance technology, actions have to go beyond vague assurances about data integrity and responsible sharing. Two approaches lend themselves to generating community trust in such situations: [220]

a) The formulation of specific legislative protections. This approach is more likely and more effective where personal data protections are already in place through law and administration, and rights to privacy and personal data integrity are recognised.

b) Resort to general ethical guidelines and principled design requirements in the creation, operation and maintenance of AI-assisted surveillance technologies and the data they produce. An ethical compliance approach will be more suitable in jurisdictions where such a self-regulatory style in governing AI is understood and accepted.

[217] 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.

[218] Haines and Stevens (n 135).

[219] Haines and Stevens (n 135).

[220] Greenleaf and Kemp (n 64).

In efforts to improve citizen inclusion and quell unease surrounding COVIDSafe, legislators made specific amendments to the Privacy Act 1998, namely the enactment of the Privacy Amendment (Public Health Contact information) Act 2020,[221] to ensure stronger statutory privacy protections for users and their collected data. The Privacy Amendment Act replaced the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020[222] which had initially provided guidelines regarding the collection, use and disclosure of COVIDSafe app data in efforts to increase public acceptance and uptake of the app.[223] The implemented legislation serves as a signal to the general public that the government has acknowledged privacy concerns and taken steps to safeguard these rights, in hopes that such citizen inclusion efforts will bolster trust in the government's policies and in turn, voluntarily cooperate in control measures.

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.[224]

2. Taiwan's collaborative approach with citizen hackers

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[225] out of its nearly 24 million citizens.[226] The low infection rates are attributed to civic co-operation, owing to the fact that digital disinformation has largely been addressed by an existing

[221] AG, 'Privacy Amendment (Public Health Contact Information) Act 2020' <https://www.legislation.gov.au/Details/C2020A00044/Html/Text, http://www.legislation.gov.au/Details/C2020A00044> accessed 3 September 2020.

[222] Health, 'Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020' <https://www.legislation.gov.au/Details/F2020L00480/Html/Text, http://www.legislation.gov.au/Details/F2020L00480> accessed 3 September 2020.

[223] 'COVID-19: Key Australian Legislation and Legislative Instruments | Practical Law' <https://content.next.westlaw.com/Document/I53a7ab38694811eaadfea82903531a62/View/FullText.html?transitionType=Default&contextData=(sc.Default)> accessed 3 September 2020.

[224] Reuters, '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.

[225] 'Coronavirus (COVID-19)' (*Google News*) <https://news.google.com/covid19/map?hl=en-SG&gl=SG&ceid=SG:en> accessed 3 September 2020.

[226] Christina Farr Gao Michelle, '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.

architecture of a “[large] digital literacy of civic engagement” implemented prior to the pandemic.[227]

Previously, the Taiwanese administration acknowledged civic disengagement and sought to remedy that by approaching a group of civic-minded hackers and coders, g0v,[228] who are devoted to improving government transparency through the creation of open-source technologies.[229] Collaboration with the government resulted in the setting up of platforms, e.g. vTaiwan[230] and Pol.is,[231] which allow for public representatives and private organizations to 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.[232] 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.[233] 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),[234] to recognise and amplify the best voices in society.[235]

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.[236] 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.[237] This enabled for public contribution of real-time stock taking, where those with masks would show up as green on the

[227] ‘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.

[228] ‘G0v.Asia’ <http://g0v.asia/> accessed 3 September 2020.

[229] Tang (n 217).

[230] ‘VTaiwan.Tw — 數位經濟法規線上諮詢’ <https://vtaiwan.tw/> accessed 3 September 2020.

[231] ‘Polis’ <https://pol.is/home> accessed 3 September 2020.

[232] Tang (n 217).

[233] 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.

[234] ‘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.

[235] ‘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.

[236] ‘Three Ways Taiwan Is Adapting to the New Normal’ (n 235).

[237] Michal Chabinski, ‘Getting Civic About Technology’ (4 August 2020) <https://www.echo-wall.eu/currents-context/getting-civic-about-technology>.

app, while out-of-stock stores would turn red.[238] 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.[239] 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.[240] 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.

The examples above have demonstrated that government-initiated efforts to include citizens in COVID control responses induce a virtuous cycle of public confidence and accountability, where citizens willingly trust and comply with the government's policies.

[238] 'How Taiwan's Unlikely Digital Minister Hacked the Pandemic' (n 227).

[239] 'How Taiwan's Unlikely Digital Minister Hacked the Pandemic' (n 227).

[240] 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.

Section 6: Conclusion and Appendix

Conclusion

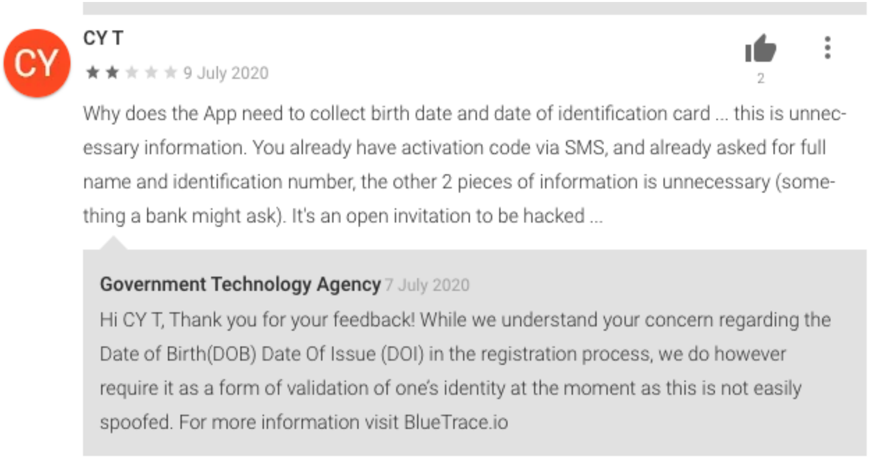
With the various applications of the AI-assisted surveillance technologies, governments and their private sector collaborators have all too often determined technologized pandemic control policies without citizen engagement or accessible public awareness investment. Trust in the government's control strategies, particularly those which depend on community involvement and compliance for efficacy is not something to be assumed as a consequence of provident state health/safety initiatives. The generation and maintenance of community trust requires similar efforts as are employed in maximising the efficacy of prevention and control technologies. Given the difficulties of balancing individual rights (however relative and contextual), such as privacy and personal data integrity, civil liberties of association, movement and speech, along with the need to safeguard public health, there has developed a regrettable policy assumption that citizens must sacrifice freedoms and protections if control and prevention efforts are to be realised. It is hoped that this paper inspires an alternative thinking. Where surveillance regimes are intrusive, and data subjects are ignorant of their reach and consequences, distrust prevails and this, more than any other variable, diminishes efficacy. It is not so much what the citizen has to forgo, but what the promoters of surveillance tech responses must elucidate, that impacts on successful policy implementation.

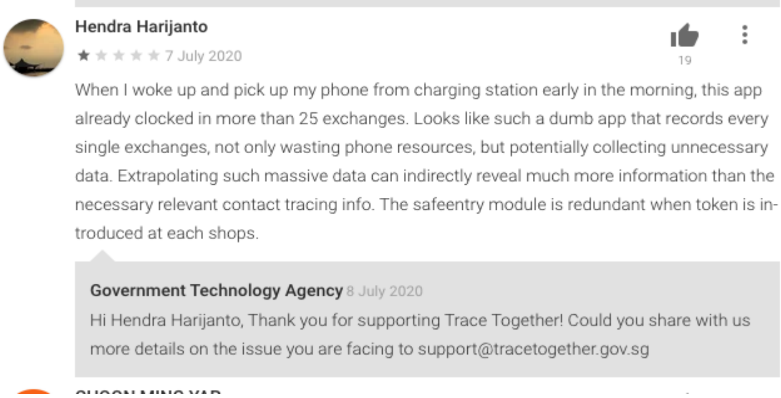
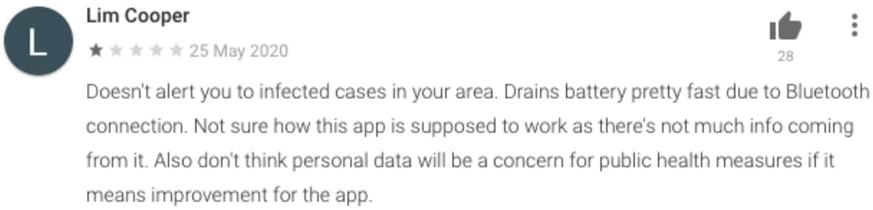
This paper has sought to provide a preliminary overview of emerging concerns, surrounding pandemic control strategies employing technology, and situate these as they are voiced within various communities grappling with their distinctly situational pandemic contexts and control realities. It is only through comprehensive and critical efforts to understand and respond to community disquiet that greater ethical compliance will be actionable beyond lofty goals. Principled design accompanied by extensive stakeholder education and engagement, rather than autocratic exercises of power and heavy enforcement, will see a more responsible location of prevention strategies within public tolerance and support. If the motivation for surveillance is targeted pandemic control and not longer term social ordering, then citizens can be brought onboard through policy transparency and operational accountability. The results of such engagement is less distrust and disquiet, more confidence and compliance and better containment outcomes.

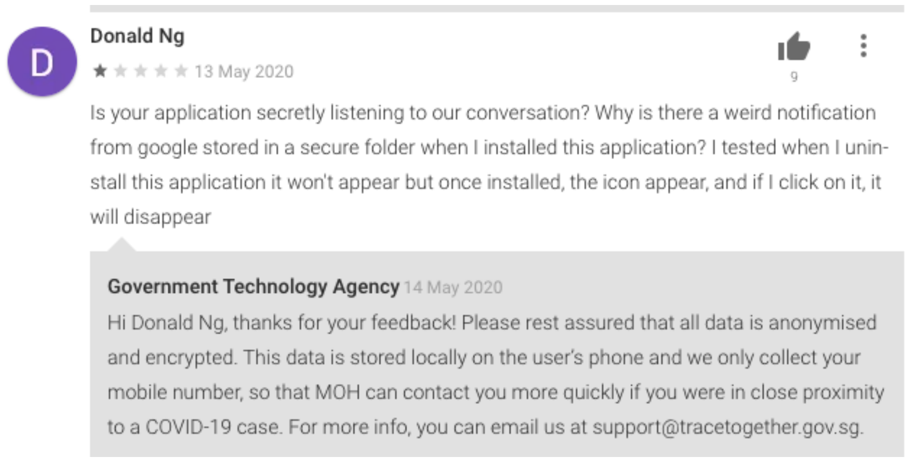
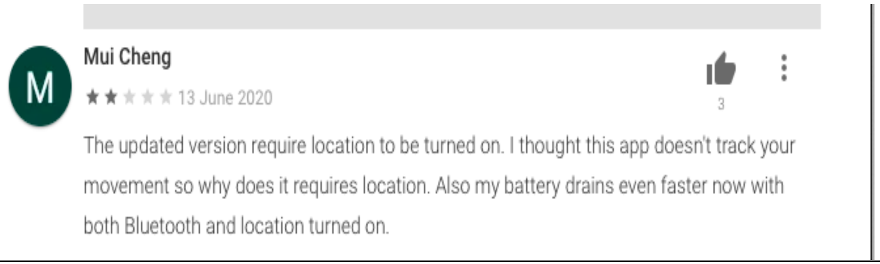
As we have shown, there is a pressing need to locate policy responses in a framework that prioritises transparency, explainability, and fairness. This framework should be implemented not only in the principled design, roll-out and review of the technology, but in communication and legislative processes as well that speak to communities currently confused about risks and consequences. As Taiwan has demonstrated, citizen inclusion is not an unattainable theoretical ideal, but an indispensable precondition in achieving voluntary compliance to eradicate the pandemic.

<u>Appendix</u>

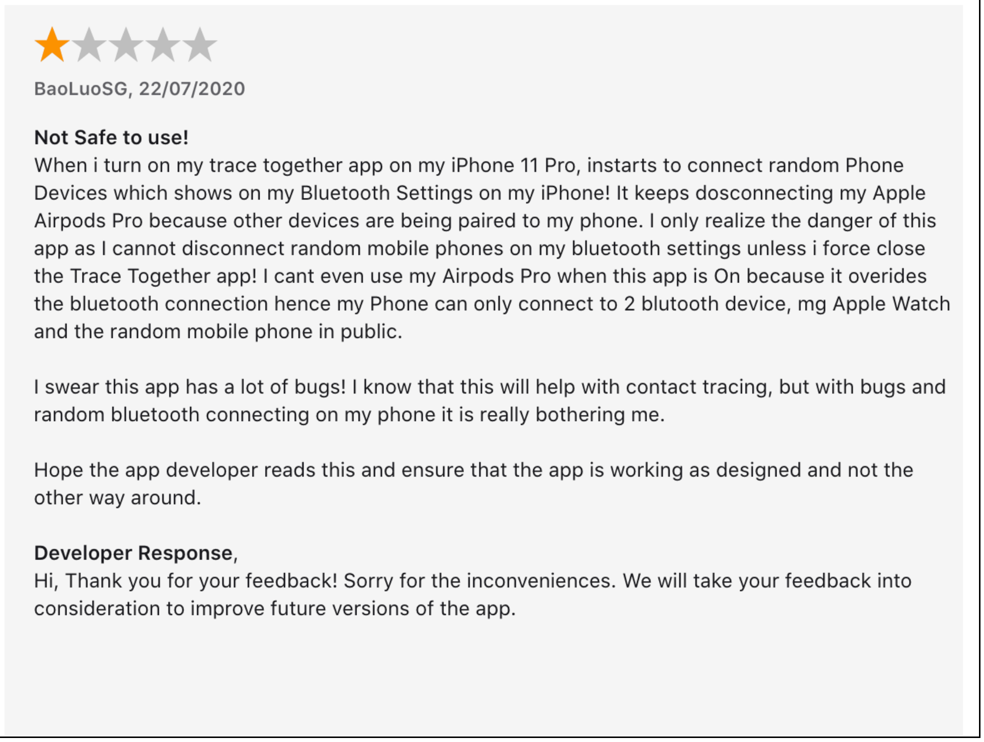
<u>Google Play Store reviews</u>

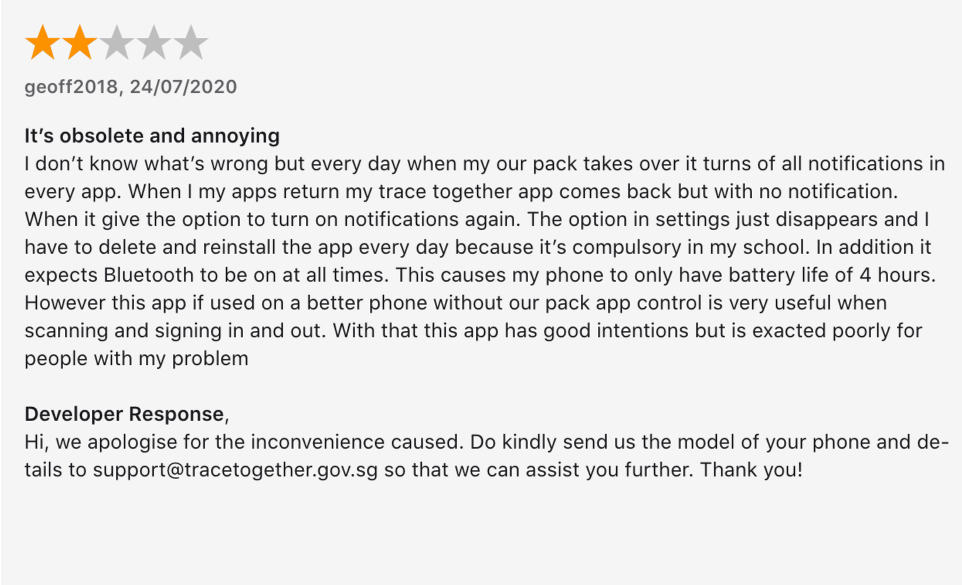
Worries and concerns posed by users	**Reviews of the TraceTogether App (and screenshots)**
• Collection of irrelevant, duplicitous or unnecessary information • Concerns of hacking	User CY T asked: Why does the App need to collect birth date and date of identification card ... this is **unnecessary information**. You already have activation code via SMS, and already asked for full name and identification number, the **other 2 pieces of information is unnecessary** (something a bank might ask). It's an **open invitation to be hacked** ...  CY T ★★☆☆☆ 9 July 2020 Why does the App need to collect birth date and date of identification card ... this is unnecessary information. You already have activation code via SMS, and already asked for full name and identification number, the other 2 pieces of information is unnecessary (something a bank might ask). It's an open invitation to be hacked ... Government Technology Agency 7 July 2020 Hi CY T, Thank you for your feedback! While we understand your concern regarding the Date of Birth(DOB) Date Of Issue (DOI) in the registration process, we do however require it as a form of validation of one's identity at the moment as this is not easily spoofed. For more information visit BlueTrace.io
• Concerns about use of mass collection of data • Lack of transparency of data use • Unsure of technological usages	User Hendra Harijanto: When I woke up and pick up my phone from charging station early in the morning, this app already clocked in more than 25 exchanges. Looks like such a **dumb app that records every single exchanges**, not only wasting phone resources, but **potentially collecting unnecessary data**. Extrapolating such massive data can indirectly **reveal much more information than the necessary** relevant contact tracing info. The SafeEntry module is redundant when token is introduced at each shops.

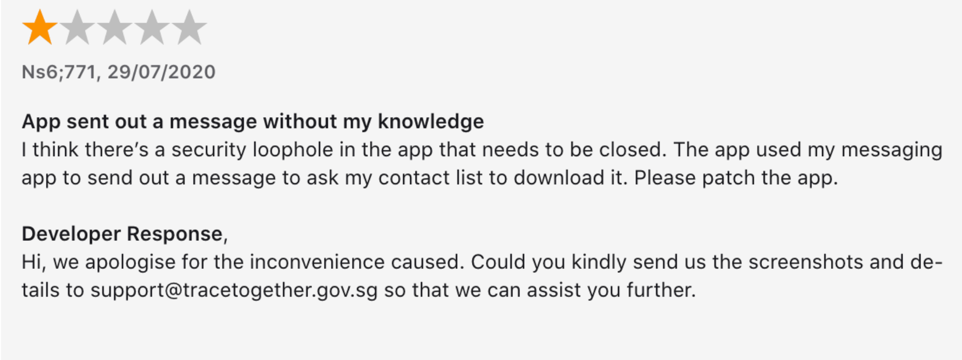
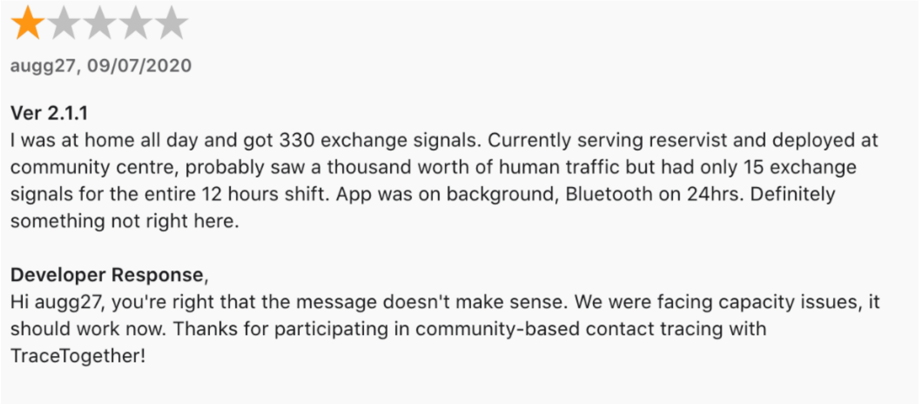
Worries and concerns posed by users	Reviews of the TraceTogether App (and screenshots)
	 Hendra Harijanto ★★★★★ 7 July 2020 19 When I woke up and pick up my phone from charging station early in the morning, this app already clocked in more than 25 exchanges. Looks like such a dumb app that records every single exchanges, not only wasting phone resources, but potentially collecting unnecessary data. Extrapolating such massive data can indirectly reveal much more information than the necessary relevant contact tracing info. The safeentry module is redundant when token is introduced at each shops. Government Technology Agency 8 July 2020 Hi Hendra Harijanto, Thank you for supporting Trace Together! Could you share with us more details on the issue you are facing to support@tracetogether.gov.sg
• Lack of transparency as to how the app is used • Expectations of presumed utility of the app not met	User Lim Cooper: **Doesn't alert you to infected cases in your area**. Drains battery pretty fast due to Bluetooth connection. **Not sure how this app is supposed to work** as there's not much info coming from it. Also **don't think personal data will be a concern for public health measures** if it means improvement for the app.  Lim Cooper ★★★★★ 25 May 2020 28 Doesn't alert you to infected cases in your area. Drains battery pretty fast due to Bluetooth connection. Not sure how this app is supposed to work as there's not much info coming from it. Also don't think personal data will be a concern for public health measures if it means improvement for the app.
• Scepticism/ distrust towards app • Response from Government Technology Agency reinforced the lack of transparency of data collection and app usage	User Ng Eric: This app should trace people who may have gone undetected. However there is **no stats to show this is working. Can we really trust** this app? Appreciate the response. Apparently, news have confirmed this is not effective as too few people are using. Perhaps should collaborate with telcos to trace using 3G/4G signals without having people to download. The new digital barcode is not accepted at Novena Square and still had to use physical nric instead. Reason given was it was "not recognisable". Government Technology Agency's reply: Due to **privacy concerns**, **we do not expose stats** if there is **<u>no real need</u>** to. "

Worries and concerns posed by users	**Reviews of the TraceTogether App (and screenshots)**
• Skepticism about app usage and paranoia	User Donald Ng: Is your application **secretly listening to our conversation**? Why is there a **weird notification** from google stored in a secure folder when I installed this application? I tested when I uninstall this application it won't appear but once installed, the icon appear, and if I click on it, it will disappear  Donald Ng ★☆☆☆☆ 13 May 2020 9 Is your application secretly listening to our conversation? Why is there a weird notification from google stored in a secure folder when I installed this application? I tested when I uninstall this application it won't appear but once installed, the icon appear, and if I click on it, it will disappear Government Technology Agency 14 May 2020 Hi Donald Ng, thanks for your feedback! Please rest assured that all data is anonymised and encrypted. This data is stored locally on the user's phone and we only collect your mobile number, so that MOH can contact you more quickly if you were in close proximity to a COVID-19 case. For more info, you can email us at support@tracetogether.gov.sg.
• Concerns about location tracking • Uncertainty about how the application is used	User Mui Cheng: The updated version **require location to be turned on**. I thought this app doesn't track your movement so **why does it requires location**. Also my battery drains even faster now with both Bluetooth and location turned on.  Mui Cheng ★★☆☆☆ 13 June 2020 3 The updated version require location to be turned on. I thought this app doesn't track your movement so why does it requires location. Also my battery drains even faster now with both Bluetooth and location turned on.

Apple App Store reviews

Worries and concerns posed by users	**Reviews of the TraceTogether App (and screenshots)**
- Concerns about Bluetooth and troubleshooting matters in relation to other Apple products	User BaoLuoSG: When i turn on my trace together app on my iPhone 11 Pro, instarts to **connect random Phone Devices** which shows on my Bluetooth Settings on my iPhone! It keeps dosconnecting my Apple Airpods Pro because other devices are being paired to my phone. I only realize the danger of this app as I cannot disconnect random mobile phones on my bluetooth settings unless i force close the Trace Together app! **I cant even use my Airpods Pro when this app is On because it overides the bluetooth connection** hence my Phone can only connect to 2 blutooth device, mg Apple Watch and the random mobile phone in public. I swear this app has a lot of bugs! I know that this will help with contact tracing, but with bugs and random bluetooth connecting on my phone it is really bothering me.  ★☆☆☆☆ BaoLuoSG, 22/07/2020 **Not Safe to use!** When i turn on my trace together app on my iPhone 11 Pro, instarts to connect random Phone Devices which shows on my Bluetooth Settings on my iPhone! It keeps dosconnecting my Apple Airpods Pro because other devices are being paired to my phone. I only realize the danger of this app as I cannot disconnect random mobile phones on my bluetooth settings unless i force close the Trace Together app! I cant even use my Airpods Pro when this app is On because it overides the bluetooth connection hence my Phone can only connect to 2 blutooth device, mg Apple Watch and the random mobile phone in public. I swear this app has a lot of bugs! I know that this will help with contact tracing, but with bugs and random bluetooth connecting on my phone it is really bothering me. Hope the app developer reads this and ensure that the app is working as designed and not the other way around. **Developer Response**, Hi, Thank you for your feedback! Sorry for the inconveniences. We will take your feedback into consideration to improve future versions of the app.

Worries and concerns posed by users	Reviews of the TraceTogether App (and screenshots)
• Poor user interface, excessive battery drain caused by prolong use of Bluetooth, lack of notifications	User geoff2018: I don't know what's wrong but every day when my our pack takes over it turns of all notifications in every app. When I my apps return my trace together app comes back but with no notification. **When it give the option to turn on notifications again. The option in settings just disappears and I have to delete and reinstall the app every day because it's compulsory in my school.** In addition it expects Bluetooth to be on at all times. This causes my phone to only have **battery life of 4 hours**. However this app if used on a better phone without our pack app control is very useful when scanning and signing in and out. With that this app has good intentions but is exacted poorly for people with my problem  ★★☆☆☆ geoff2018, 24/07/2020 **It's obsolete and annoying** I don't know what's wrong but every day when my our pack takes over it turns of all notifications in every app. When I my apps return my trace together app comes back but with no notification. When it give the option to turn on notifications again. The option in settings just disappears and I have to delete and reinstall the app every day because it's compulsory in my school. In addition it expects Bluetooth to be on at all times. This causes my phone to only have battery life of 4 hours. However this app if used on a better phone without our pack app control is very useful when scanning and signing in and out. With that this app has good intentions but is exacted poorly for people with my problem **Developer Response**, Hi, we apologise for the inconvenience caused. Do kindly send us the model of your phone and details to support@tracetogether.gov.sg so that we can assist you further. Thank you!
• Unauthorised use of sharing within the app to other contacts within the phone • Privacy concerns • Uncertainty about how the app is being used	User Ns6;771: **App sent out a message without my knowledge** I think there's a **security loophole in the app** that needs to be closed. The app used my **messaging app to send out a message** to ask my contact list to download it. Please patch the app.

	 ★☆☆☆☆ Ns6;771, 29/07/2020 **App sent out a message without my knowledge** I think there's a security loophole in the app that needs to be closed. The app used my messaging app to send out a message to ask my contact list to download it. Please patch the app. **Developer Response**, Hi, we apologise for the inconvenience caused. Could you kindly send us the screenshots and details to support@tracetogether.gov.sg so that we can assist you further.
Worries and concerns posed by users	**Reviews of the TraceTogether App (and screenshots)**
- Uncertainty about how the app works, incorrect or inefficient tracking information	User augg27: I was at home all day and got 330 exchange signals. Currently serving reservist and deployed at community centre, **probably saw a thousand worth of human traffic but had only 15 exchange signals for the entire 12 hours shift**. App was on background, Bluetooth on 24hrs. Definitely something not right here.  ★☆☆☆☆ augg27, 09/07/2020 **Ver 2.1.1** I was at home all day and got 330 exchange signals. Currently serving reservist and deployed at community centre, probably saw a thousand worth of human traffic but had only 15 exchange signals for the entire 12 hours shift. App was on background, Bluetooth on 24hrs. Definitely something not right here. **Developer Response**, Hi augg27, you're right that the message doesn't make sense. We were facing capacity issues, it should work now. Thanks for participating in community-based contact tracing with TraceTogether!