Volume **3** (1) 2021 https://doi.org/10.5204/lthj.1808

Implementing COVIDSafe: The Role of Trustworthiness and Information Privacy Law

Mark Burdon and **Brydon Wang**
Queensland University of Technology, Australia

Abstract

Governments worldwide view contact tracing as a key tool to mitigate COVID-19 community transmission. Contact tracing investigations are time consuming and labour intensive. Mobile phone location tracking has been a new data-driven option to potentially obviate investigative inefficiencies. However, using mobile phone apps for contact tracing purposes gives rise to complex privacy issues. Governmental presentation and implementation of contact tracing apps, therefore, requires careful and sensitive delivery of a coherent policy position to establish citizen trust, which is an essential component of uptake and use. This article critically examines the Australian Government's initial implementation of the COVIDSafe app. We outline a series of implementation misalignments that juxtapose an underpinning regulatory rationality predicated on the implementation of information privacy law protections with rhetorical campaigns to reinforce different justifications for the app's use. We then examine these implementation misalignments from Mayer and colleagues' lens of trustworthiness (1995) and its three core domains: ability, integrity and benevolence. The three domains are used to examine how the Australian Government's implementation strategy provided a confused understanding of processes that enhance trustworthiness in the adoption of new technologies. In conclusion, we provide a better understanding about securing trustworthiness in new technologies through the establishment of a value consensus that requires alignment of regulatory rationales and rhetorical campaigning.

***Keywords**:* Contact tracing apps; COVIDSafe; information privacy law; trustworthiness.

Introduction

The World Health Organization noted at the onset of the COVID-19 pandemic that contact tracing was "the backbone" of successful governmental response.[1] The importance of contact tracing for pandemic management has historically been recognized as an important but time-consuming and laborious exercise.[2] COVID-19 is largely transmitted through direct or proximate human-to-human connection. Contact tracing activities consequently involve numerous interviews that retrace the recent location histories of positively identified individuals to ascertain potential sources of transmission. Governments across the globe have turned to mobile phone location tracking[3] as a new data-driven option to obviate investigative inefficiencies. Mobile phone contact tracing is potentially important because it can provide data, with relative ease, of the previous location histories and possible closeness of positively identified individuals to other individuals. This allows contact tracing to be carried out more efficiently to stem the tide of potential waves of transmission.[4]

A range of mobile phone contact tracing strategies has been developed during the pandemic. These involve differences relating to the collection of mobile phone metadata. For example, some schemes only collected Bluetooth data,[5] whereas others collected a broader range of data from the many location sensors used in a mobile phone.[6] A key difference also involved the

[1] World Health Organization, "Opening Remarks."
[2] European Centre for Disease Prevention, Contact Tracing for COVID-19.
[3] Morley, "Ethical Guidelines"; Lodders, "Scrutinising COVIDSafe," 155.
[4] Ivers, "Lost Time."
[5] Ahmed, "Contact Tracing Apps," 6.
[6] Ryan, "Digital Contact-Tracing," 384.

use of mandatory and voluntary schemes. In some countries, such as Israel, some contact tracing apps were mandated by emergency legislation to obviate information privacy law protections that would normally prohibit such data collections and transfers.[7] Conversely, voluntary schemes were opt-in and involved active forms of consent to offer stronger forms of information privacy protection.[8] Similarly, differences arose between individualized and aggregated outcomes. Some schemes provided highly individualized outputs, which can be used to monitor the current location of COVID-19 positively identified individuals who are required to self-quarantine.[9] Other schemes provided aggregated, hotspot visualizations of locations where positively identified individuals were known to have been to allow other members of the public to self-check their potential exposure to COVID-19.[10]

The differences in strategic approach highlight distinct political considerations towards information privacy law. Contact tracing apps that collect a significant amount of mobile phone location data raise information privacy concerns. If combined with a relatively mandatory approach, and intended to produce highly individualized outputs, these concerns greatly increase. However, contact tracing apps that have stronger information privacy protections still give rise to public concern.[11] Public concerns are important, particularly in relation to voluntary schemes, because information privacy has been foundationally linked to higher levels of citizen uptake.[12] An intrinsic connection unfolds. Citizen trust is needed to encourage voluntary uptake, and trust is largely predicated on traditional citizen understanding of information privacy law protections.[13] As such, successful implementation was based on a circular reinforcement that equates the acquisition of citizen trust as a corollary to enhanced legal protections.[14]

This article examines the implementation strategies adopted by the Australian Government in its roll out of the COVIDSafe contact tracing app.[15] COVIDSafe adoption was voluntary and its implementation was supported by dedicated legislation ("the *COVIDSafe Act*").[16] The *Privacy Act 1988* (Cth) ("*Privacy Act*") was amended to provide stronger information privacy protections solely for contact tracing purposes. However, despite a strong initial interest,[17] the overall uptake numbers were disappointing and did not meet the government's intended target.[18] The lack of uptake gives rise to critical questioning about the government's implementation strategy and the accepted relationship between information privacy law protections and the establishment of citizen trust.

To do so, we adopt Mayer and colleagues' framework of trustworthiness[19] to identify implementation misalignments between the regulatory rationales and the rhetorical campaigns employed to promote the app. From a trustworthy perspective, Australian citizens are trustors who provide their trust, and the Australian Government is a trustee that seeks to receive the trust accorded from its citizens. The Mayer framework examines the characteristics of trustworthy actions that promote trust across three domains: ability, integrity and benevolence. Ability involves trustee competencies that enable the completion of tasks necessary to influence the trustor. For this article, competencies involve the technical and legal actions of the Australian Government exhibited in COVIDSafe implementation. Integrity regards value congruence and entails acts that seek to align the value sets of the trustor and the trustee. Value congruence in this article regards willing compliance with information privacy law requirements by the Australian Government and citizens. Finally, benevolence regards the overall disposition of the trustee to

[7] Winer, "Health Ministry." Note the initial mandatory nature of the app was withdrawn following legal action. See Lodders, "Scrutinising COVIDSafe," 155; Greenleaf, "Phase II," 5 for other country examples.
[8] Morley, "Ethical Guidelines."
[9] Briefing, "Countries Are Using Apps."
[10] Ahmed, "Contact Tracing Apps."
[11] Couch, "Extending Surveillance."
[12] Kretzschmar, "Impact of Delays," 458.
[13] Bell, "What Motivates People," 4–5. As Bell and colleagues highlight, privacy is an important consideration, but it is not the only consideration relevant to the broader discussion about trust establishment in contact tracing apps. Other important issues outlined by Bell and colleagues, and the other authors cited in this paper, include effective public health messaging, digital divides across communities, technical issues of usability and interoperability, and individual motivations and willingness to provide data generally to government. However, for the purposes of this article, we focus on the information privacy issues relevant to the implementation of the COVIDSafe app, given the importance attached to these types of protections by the Australian Government in its COVIDSafe implementation strategy. We nevertheless acknowledge that several other key issues are at play regarding the establishment of trust, but we believe the focus on information privacy is relevant given its central positioning as part of the Australian Government's attempt to engender citizen trust through the implementation of specific COVIDSafe legal protections.
[14] Greenleaf, "Australia's COVIDSafe App," 2.
[15] We agree with Greenleaf and Kemp that the app is really a "COVIDSafe system" that involves multiple entities. See Greenleaf, "Phase III," 14.
[16] *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth).
[17] Worthington, "Chief Medical Officer."
[18] Galloway, "The COVID Cyborg," 165 describing the modelling behind projected uptake targets as "arbitrary."
[19] Mayer, "Integrative Model."

"do good" for the trustor. In COVIDSafe, benevolence is about seeking value consensus that underpins ability and integrity actions. A benevolent disposition is signalled through the overarching policy basis for COVIDSafe implementation. The policy basis provides focus on how information privacy law protections and technical requirements are implemented through regulatory rationales and rhetorical campaigning.

We argue that an ideal COVIDSafe implementation strategy would have aligned the three domains of trustworthy actions and was consistent in implementation delivery. However, as detailed in this paper, we do not believe the Australian Government was able to achieve this alignment in either respect. Before we get that far, we first outline the COVIDSafe implementation strategy, and highlight the misalignments between the approaches of regulatory rationality and rhetorical campaigning employed in the roll out.

Implementing COVIDSafe

The COVIDSafe roll out started in April 2020 at a heightened time of uncertainty about widespread community transmission throughout Australia. The first wave of the pandemic had reached world shores and initial reports suggested that preventative responses from Asian governments were stemming the tide of transmission. It is perhaps not surprising, then, that the Australian Government largely adopted the Singaporean contact tracing app, TraceTogether,[20] as the model for its own technological solution. COVIDSafe is a voluntary, Bluetooth-based data collection app that collects data about a user's[21] proximity to another mobile phone that has the app downloaded on it.[22] Data of the second phone were recorded but only analyzed if the phone were in a proximate distance of 1.5 metres from the user's phone for a period of 15 minutes or more.[23] If a user tested positive for COVID-19, the user then uploaded their COVIDSafe app data to a central database depository, and the data were distributed to the relevant state-based contact tracing authority.

Even though the adoption of COVIDSafe was based on the Singaporean contact tracing app,[24] there were some significant differences between the two apps, in terms of design, application and especially in intended and actual data use. The registration data required for downloading and using the COVIDSafe app were significantly greater than TraceTogether.[25] Centralized contact tracing apps,[26] such as COVIDSafe and TraceTogether, require the generation of unique identifiers, managed and issued by a central authority, that can be related back to an individual user.[27] However, TraceTogether generated a separate temporary identifier that was exchanged with other mobile phone users, whereas COVIDSafe exchanged encrypted personal information about users that could later be decrypted by public health officials.[28] Most importantly, the use of TraceTogether data occurred in significantly broader ways by the Singaporean Government compared to its Australian counterpart. TraceTogether data were used to track and monitor the movements of migrant workers who were deemed to reside in higher risk environments, such as dormitories.[29] TraceTogether data could also be legally used by law enforcement agencies where there is a "clear and pressing" need for criminal investigations relating to seven categories of serious criminal offence.[30] The *COVIDSafe Act* specifically prohibited such types of law enforcement access and use.[31]

These differences underlie some of the different democratic structures in operation in Australia and Singapore. Goggin rightly highlights the different privacy histories in both jurisdictions, comparing the relative infancy of Singaporean legal protections

[20] Bennett Moses, "COVIDSafe," 497; Goggin, "COVID-19 Apps," 63.
[21] A user is a person who has voluntarily downloaded the app on to their phone. See Greenleaf, "Australia's COVIDSafe App," 3.
[22] Greenleaf, "Phase II," 4 noting that proximity is not defined but for incorrect "ministerial explanations."
[23] It should be noted that the issue of data processing turned into a controversial point, as analysis of time and proximity was conducted centrally rather than on the phone itself. Therefore, all data had to be uploaded before it could be determined whether it would fit within the time and proximal parameters. See Greenleaf, "Australia's COVIDSafe App," 11.
[24] Goggin, "COVID-19 Apps," 65.
[25] COVIDSafe registration required the provision of name, mobile number, age and postcode, whereas TraceTogether only required a mobile number first instance.
[26] In terms of the limitations of the paper's analysis, we acknowledge that there is a significant and important debate about the privacy and surveillance implications that arise from the use of centralized or decentralized frameworks. See Leins, "Tracking," 7. Our paper solely focuses on the use of centralized systems, such as COVIDSafe and TraceTogether, but we acknowledge that a different type of trustworthy debate would arise in relation to government contact tracing apps based on a decentralized system. As Leins and colleagues note, the use of different contact tracing models "reflect[s] differing societal priorities" regarding individual and societal-based privacy protections.
[27] Leins, "Tracking," 6.
[28] Alanzi, "A Review of Mobile Applications," 52.
[29] Goggin, "COVID-19 Apps," 68.
[30] Chee, "S'pore Govt to Pass Law."
[31] Greenleaf, "COVIDSafe Law for Contact Tracing."

of information privacy with the longer Australian experience.[32] It is also important to note how TraceTogether data were incorporated into a broader centralized Singaporean focus of "Smart Nation" policies,[33] which certainly is not as strong in Australia's federated system. As such, even though the Singaporean and Australian apps are largely based on the same technical framework, the underpinning governmental and administrative systems that underlie its use are different, and this had significant effects, particularly on Australian legislative and regulatory considerations.

The structure of Australia's federated system required a much greater focus on the ostensible basis of regulatory rationality underpinning the COVIDSafe implementation strategy. By regulatory rationality, we mean the instrumental application of information privacy law as the predominant means of establishing citizen trust in the use of the COVIDSafe app. The focus of instrumentality is the process protections that emanate through information privacy law, and were enhanced by the enacting framework of the COVIDSafe legislation to further engender citizen trust. The instrumental basis and the focus of process protections manifest in the specific requirements of information privacy law and the singular types of protection that it seeks to provide. For the purposes of this paper, we focus on one requirement, Australian Privacy Principle (APP) 3.5 and the obligation to collection personal information in a lawful and fair manner.[34] We use APP 3.5 because the legislative requirement for fair and lawful collections highlights the differences in implementation approach between regulatory rationality as a means of engendering citizen trust, on the one hand, and the rhetorical campaigns used to promote COVIDSafe to the public and raise its uptake by citizenry as a moral imperative, on the other. Table 1 outlines the differences in approach.

Table 1. COVIDSafe Implementation Strategy and Juxtapositions of Regulatory Rationality and Rhetorical Campaigns

Implementation strategy	**Regulatory rationality**	**Rhetorical campaigns**
Basis	Instrumentality	Emotionality
Focus	Process protections	Relational acts
Requirement	Lawful	Fair

Basis: Instrumentality v Emotionality

We contend that legal instrumentality is the basis of regulatory rationality behind the COVIDSafe implementation strategy. The fragmented nature of Australia's information privacy law regime has conceptually similar laws at Commonwealth and state/territory levels.[35] However, these laws apply in different ways,[36] which meant that the implementation of the COVIDSafe app had to be undertaken through legislative changes to the *Privacy Act* for it to be lawful. The Australian Government, through a combination of different agencies,[37] purported to be the data collector of COVIDSafe data. It merely provided the legal and technical infrastructure for data transfers to state-based contact tracing authorities.[38] The Australian Government through Amazon Web Services provided the pipes for data to flow from users, and then to the state-based contact tracing authorities. Here is where the problem of fragmentary legal coverage arose.

The *Privacy Act* only covers Australian Government agencies and certain private sector organizations. South Australia and Western Australia do not have information privacy laws that govern the handling of personal information by their state agencies.[39] The application of information privacy in states that have such laws, like New South Wales, Victoria and Queensland, is subtly different.[40] Therefore, unlike Singapore, guaranteeing a level playfield of information privacy protection

[32] Goggin, "COVID-19 Apps," 70. Note Singapore's first comprehensive data protection law was introduced in 2012 compared to the introduction of the *Privacy Act* in 1988, albeit with a limited focus on Australian Government and ACT agencies.
[33] Goggin, "COVID-19 Apps," 70.
[34] The issue of fair and lawful collection is by no means the only information privacy issue to arise from COVIDSafe implementation. Our focus is limited to Australia Privacy Principle (APP) 3.5 because we believe it highlights some fundamental disconnects in implementation approach. For a clear illustration of the broader issues arising from the *Privacy Act 1988* (Cth), see the in-depth analysis of Greenleaf and Kemp cited in this article.
[35] Greenleaf, "Privacy in Australia."
[36] Australian Law Reform Commission, Serious Invasions, 41.
[37] The Department of Health were deemed the COVIDSafe data custodian and the Department of Media, Communications and Sport were deemed the infrastructure providers. See Maddocks, "Privacy Impact Assessment."
[38] Maddocks, "Privacy Impact Assessment," 56; Greenleaf, "Phase II," 19.
[39] Office of the Australian Information Commissioner, "Privacy in Your State."
[40] Australian Law Reform Commission, "For Your Information," 164.

for users throughout Australia is a complex legal challenge.[41] Consequently, it is again perhaps not surprising that the initial implementation focus was so heavily predicated on the provision of instrumental legal protections to garner citizen trust. However, the unfurling of COVIDSafe's trust-engendering legal instrumentality came in combination with a barrage of rhetorical campaigns driven from the highest heights of the Australian Government. The campaign included media comments by the prime minister, and other key government ministers, and population scale advertising in traditional and social media outlets.

The fact that the Australian Government chose to publicly highlight COVIDSafe is not surprising, especially given the uncertainty of transmission at the time of its unveiling. What is surprising is the choice of rhetorical targeting as a base for the campaign.[42] Floreani has helpfully identified three components to the government's COVIDSafe public relations campaign. First is the government's use of "wartime" language to promote a heightened state of emergency.[43] Its rhetorical purpose is twofold—to bind the country together and to prepare citizenry for the necessary social, legal and technical changes required to "fight the virus."[44] Thus, downloading the app is part of a wartime effort akin to "national service."[45] Second, and flowing from the first component, is the "Team Australia"[46] imperative, which again serves a twofold purpose. First, this continues binding citizenry together, this time under the patriotic flag of sporting mateship. Second, it reiterates the collective necessities required for Australia to return to "normal."[47] Therefore, downloading the app will get Australian citizens "back to the footy."[48] Third, and flowing from the previous two components, is the app's use as an individual and collective form of protection. Downloading the app is "sunscreen" that helps to protect "you," "your family," "your loved ones" and your "nation."[49]

Floreani rightfully highlighted the "terrible brilliance" of this combined approach because it framed the implementation and individual downloading of COVIDSafe by citizens as a "question of morality."[50] It is a matter of civic duty and "the right thing to do" because downloading the app will save the lives of other Australians and help to preserve the Australian way of life.[51] Needless to say, all of these moral incantations are questionable, not least because of the limited purposes for which Bluetooth mobile data can reasonably be used.[52] More importantly, though, for the purposes of this paper, is the juxtaposition between the regulatory rationality of the implementation strategy and the rhetorical campaigning applied. The former seeks to engender citizenry trust in COVIDSafe predominantly through enhanced information privacy law protections. The latter seeks to morally compel the use of COVIDSafe through emotionally imposing reasons. Thus, the basis of the COVIDSafe implementation strategy is, on its face, misaligned. We outline further in this paper, but note also for now, how the misaligned fusion of instrumentality and emotionality as the basis of the strategy does not signal the type of benevolent disposition that promotes trustworthiness.

Focus: Process Protections v Relational Acts

The focus elements of implementation shift attention from the basis of the overall strategy to how the strategy was to be achieved. We contend there is a better alignment of expected outcomes in how COVIDSafe is implemented, albeit from different perspectives. The focus of regulatory rationality is enhancements to the pre-existing processes of principled protection that pervade the logics and application of information privacy law in the *Privacy Act*. The focus of rhetorical campaigning is the reinforcement of civic and moral duties on Australian citizens to protect each other. Points of regulatory and rhetorical intertwinement are reached because legislative protections and government media campaigns focus on how Australian citizens relate to each other in the context of COVIDSafe data provision. Key to this greater alignment is the notion of trust that pervades structures of individual control regarding the provision of personal information.[53]

Information privacy law provides a range of life cycle, largely processual protections, which begin at the point of data collection and end with destruction or de-identification of no longer required data.[54] In the interim, data collection organizations have a

[41] Greenleaf, "Phase II," 11.
[42] Greenleaf, "Australia's COVIDSafe App," 15.
[43] Floreani, "Navigating," 33.
[44] Goggin, "COVID-19 Apps," 66.
[45] Goggin, "COVID-19 Apps," 66.
[46] Meade, "Australian Coronavirus."
[47] Brinsden, "COVIDSafe App."
[48] Smith, "Ministers."
[49] Floreani, "Navigating," 35.
[50] Floreani, "Navigating," 33.
[51] Goggin, "COVID-19 Apps," 66.
[52] Landau, "Location Surveillance."
[53] Bell, "What Motivates People."
[54] Bygrave, "Data Protection Law."

range of obligations to fulfil. The individual is notified about the purposes of collection so they can meaningfully consent to subsequent uses.[55] Personal information can generally only be used for a defined purpose about which the individual is adequately informed.[56] Individuals have a range of interaction mechanisms that seek to ensure the maintenance of control by being able to affirm the accuracy and currency of collected personal information.[57] Once collected and stored, personal information must be kept secure.[58] The weaknesses of the Australian information privacy law system, as exemplified through the APPs, are well documented.[59] Given the underlying trust-engendering role underpinning the COVIDSafe legislation, it is not surprising that implementation focused on strengthening existing protections.[60]

For example, section 94D of the *COVIDSafe Act* ensures that COVIDSafe app data can only be collected, used and disclosed for the purposes of undertaking contact tracing.[61] APP 3 and APP 6, which govern collections and uses/disclosures of personal information, have some broad-ranging exemptions that allow personal information to be used beyond the primary purpose of collection.[62] Therefore, the restriction of COVIDSafe app data for contact tracing is a marked protective improvement. More importantly, section 94D(1) provides that it is a criminal offence with a maximum sentence of five years' imprisonment for collecting, using or disclosing COVIDSafe app data for non-contact tracing purposes. The use of criminal sanctions for information privacy law is rare in Australia. The introduction of information privacy-related criminal offences, such as section 94D(1) of the *COVIDSafe Act*, demonstrates the perceived importance of privacy protections as a means of engendering citizen trust.[63] Similarly, much has been made of the unsatisfactory state of affairs regarding the *Privacy Act*'s definition of personal information following the full Federal Court decision of *Privacy Commissioner v Telstra*.[64] Again, the *COVIDSafe Act* provides added protections for data collected by the app through the application of the broader General Data Protection Regulation definition of personal data,[65] thus, ensuring all data collected by the app are covered by the Act. Finally, section 94X specifically regards the fragmentation issue highlighted above, and classes state or territory contact tracing authorities as "organisations."[66] The inclusion of these tracing authorities extends information privacy protections accorded by the Australian Government for COVIDSafe data purposes to all states, confirmed by agreements between states and the Commonwealth.[67]

From the perspective of regulatory rationality, the legislative changes place higher and more restrictive obligations on collectors and users of COVIDSafe app data to engender citizen trust in collection processes and ultimate uses. Crossovers with rhetorical campaigning also emerge regarding the voluntary use of the app and prohibitions on coercion. For example, section 94H prohibits the forced downloading of the app by an employer regarding an employee for entry to, or use for, work, and it prevents venue operators from making installation of the app a condition of entry.[68] The legislative confirmation of voluntary application and the prohibitions against coercive use are important additions to the traditional information privacy law framework. These safeguards are inherently relational in nature, as they move information privacy protections beyond restrictive notions of privacy based solely on the management of personal information to consider more broadly the social contexts of information exchange and the reinforcement of societal expectations about acceptable data uses.[69] Acceptability, in this sense, moves beyond data processes to how we relate to each other as exchangers, and to uses of individually and societally generated data. Informational privacy consequently has an environmental capacity[70]—a physical component, such as where someone can be denied venue entry based on not having an app.[71]

[55] Under the *Privacy Act 1988* (Cth), this is the purpose APP 3 and APP 5.
[56] The general requirement of APP 6 is that personal information can only be used for the purposes for which it is collected. However, several exemptions exist to this general requirement. See Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, and the discussion that flows from section 6.14 onwards.
[57] APP 10 obligates requirements regarding accuracy of personal information. See also the use of APP 12 and APP 13 regarding access and correction mechanisms for individuals.
[58] Under APP 11, an APP entity must take reasonable steps to protect personal information from misuse, interference and loss, including unauthorized access, modification and disclosure.
[59] Greenleaf, "Privacy in Australia"; Greenleaf, "'Tabula Rasa'."
[60] Greenleaf, "Phase III," 4.
[61] *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth) s 94D.
[62] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines.
[63] Explanatory Memorandum, *Privacy Amendment (Public Health Contact Information) Bill 2020* (Cth) s [2], 4.
[64] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4.
[65] *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth) s 94Q. See Greenleaf, "Phase II," 12–13.
[66] Under section 6 of the *Privacy Act 1988* (Cth), APP entities are regulated as agencies, in the Commonwealth public sector and organizations in relation to private sector coverage.
[67] Greenleaf, "Phase III," 13.
[68] *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth) s 94H.
[69] Nissenbaum, Privacy in Context; Cohen, "Turning Privacy."
[70] Cohen, "What Privacy Is For."
[71] McDonald, "The Digital Response."

Given the off-kilter regulatory and rhetorical perspectives that typified the basis of the implementation strategy, there is a surprisingly closer correspondence about how key implementation outcomes were to be achieved. The rhetorical campaigning focused strongly on the voluntary nature of downloading an app, and so there was a greater alignment between regulatory rationality and rhetorical campaign.[72] In other words, there was a derived meeting point generated by the *COVIDSafe Act* based on the extension of process-focused to relationally oriented information privacy law protections. Moreover, the government's rhetorical campaign at this point focused heavily on the protective benefits arising from the *COVIDSafe Act*, such as the restrictions in the uses of data for contact tracing purposes only by state authorities.[73] However, even though there is greater correspondence, there is still a heavy moral component attached to the rhetorical delivery. While the decision to download the app was "entirely voluntary," the government continued to press the case that it was the "right thing" to do[74] "when it comes to the economy and the functioning of our society."[75] The type of moral underpinning regards the re-emphasis of the "Team Australia" component and the downplaying of wartime rhetoric. However, the coercive undertones of moral compulsion are nonetheless identifiable. These undertones are important to consider when examining the legal requirements entailed in the strategy, as regulatory rationality and rhetorical campaigning are once again in disjuncture, especially through the application of APP 3.5.

Requirements: Lawful v Fair

We have highlighted that the *COVIDSafe Act* was a necessary starting point to confirm the legality of app data collections. Part of the reason for this starting point is the legal requirement for collections of personal information to be lawful and fair under APP 3.5.

As noted, a significant degree of regulatory emphasis was placed on the legality of COVIDSafe collections as a necessary requirement to overcome the challenges of a fragmented information privacy law regime. The lawful element of APP 3.5 encapsulates the reasons why. Acts that are lawful and fair are undefined in the *Privacy Act*. That said, a lawful collection is generally easier to identify, as it is one that is not prohibited by law. Law in this sense can be a statute, a regulatory rule, civil wrong or a court order.[76] A fair collection is more abstract and is oddly expressed in the negative as one that does not involve intimidation or deception, or one that is not unreasonably intrusive.[77] What is an unfair or a fair collection is inherently contextual. It depends on the circumstances of each individual collection. Generally, a covert collection involves deception so it is more likely to be unfair.[78] However, some covert collections in certain contexts may be required, such as in benefit or fraud investigations, where to notify the individual about the collection would defeat its purpose.[79] In these circumstances, it could be reasonable for a seemingly unfair collection to be fair.

We raise the issues of lawful and (un)fair collections to highlight the counter-intentional effect of disparate regulatory and rhetorical approaches. The application of unfairness as the basis for a collection principle has important consequences because it makes it easier to extend regulatory application beyond process. Fairness, as deception, intimidation, covertness or unreasonable intrusiveness, extends the regulatory focus beyond information exchange process points to broadly consider the actions of data collectors as part of their relations with individual personal information providers.

However, at this juncture, rhetorical attempts at framing COVIDSafe adoption by citizens as "the right thing to do" suddenly takes on a different connotation, as the clearer borderline between moral compulsion and what could constitute an unfair collection begins to blur.[80] The purpose of APP 3.5 is also important to consider at this point. Fairness, as a requirement of personal information collection, is legislative recognition of the power asymmetries inherent in the relationship between individuals and data collectors.[81] These asymmetries are deeply embedded in the governmental context of information privacy law's application given the ability of governments to mandate collections of personal information, much like the *COVIDSafe*

[72] Hayne, "Coronavirus App."
[73] Department of Health, "COVIDSafe: New App."
[74] Hayne, "Coronavirus App."
[75] "Scott Morrison," para. 6.
[76] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, s 3.60.
[77] Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, s 3.62.
[78] *N and Law Firm* [2011] AICRMN 8.
[79] *Griffiths v Rose* [2011] FCA 30.
[80] As noted in this paper, we use "unfair collection" in a defined information privacy context, particularly in relation to how it is interpreted specifically by the Privacy Commissioner. Therefore, a lack of fairness is understood as activities that could be construed as intimidating, deceptive or unreasonably intrusive. See Office of the Australian Information Commissioner, Australian Privacy Principles Guidelines, s 3.62. Thus, the key component of unfairness in this context relates to information asymmetries and collections of personal information. As such, there is a spectrum in which moral compulsion could be perceived as intimidation in a collection context.
[81] Clifford, "Data Protection," 144–145.

Act. The expression of power as legally mandated data collections is a purview governmental quality—a quality that requires judicious exercise of fairness, given that the executive source of power, the government, has the means of deriving lawfulness through statutory implementation through the legislative process. In an emergency situation, of course, those "means" manifestly increase for governments, such as the ability to enact law outside the full legislative process, like the first iteration of the *COVIDSafe Act*, which was authorized by a determination and without full parliamentary scrutiny.[82] A different area of compulsion is also evident, albeit at the state level of government. The enforced use of QR code registration for venue attendance has been common across Australia.[83]

We contend that the fairness component is vital to consider regarding regulatory and rhetorical attempts to engender trust in the adoption of new governmental forms of data collection. It points to a complex area of information privacy law that is conceptually thin in Australia to the extent that it is almost absent in application,[84] but is resoundingly constructed as "proportionality" in other jurisdictions, particularly in the European context.[85] Thus, the application of fairness harks to a value consideration that goes beyond instrumental application of information privacy law's process protections to the broader construct of relational acts involved in data collections, including the rhetorical campaigns of government. Engendering trust in new data collection processes is not purely an instrumental action of regulatory rationality. It involves securing a value consensus[86] based on open dialogue that explicitly signals trustworthiness, particularly as a benevolent act. To understand why that is the case, it is important to consider these issues from a trustworthiness, rather than trust, perspective.

Trust as a Matter of Trustworthiness

The role of trust and COVIDSafe implementation has been recognized as key by recent authors.[87] These detailed works highlight and cement the relationship between information privacy law protections and trust in the technical systems that are accorded protections. To examine the different regulatory rationales and strategic rhetoric deployed to enhance trust in the COVIDSafe app, we need to consider two aspects. First is the concept of trust that is trying to be enhanced, and second is the antecedent elements of trustworthiness at play in regulatory and rhetorical actions to engender trust in the app.

To think about the first question we utilize McKnight and colleagues' six concepts of trust.[88] "Trusting intention" regards the willingness of the person giving trust (the "trustor") to accept the risk of a decision to trust being wrong. The second concept, "trusting behaviour," considers the extent to which intention exhibits as actual behavioural dependency on the recipient of trust (the "trustee"). "Trusting beliefs" focus on the person doing the trusting and their cognitive beliefs about the qualities of the trustee. "System trust" considers the institutional structures, described as "impersonal structures," that provide context to trust relationships. "Dispositional trust" outlines the tendency of the trustor to give trust in generalized circumstances and categories of persons. Finally, the "situational decision to trust" addresses an intention on the part of a trustor to trust in each context.

On its face, system trust is the most relevant concept in our discussion on the types of institutional and technological structures that may lead a citizen as a trustor to reallocate their trust to the COVIDSafe app. System trust, as Keymolen and Voorwinden highlight, is a way of understanding the complex effect of technology on trust relations that entail the transfer of interpersonal trust strategies to technological systems.[89] Consequently, it is challenging and problematic to entirely separate system trust from interpersonal trusting intention. The examination of regulatory rationales and campaigning rhetoric underpinning implementation of the COVIDSafe app require both. Regulatory and rhetorical strategies have a systems-focused outcome, but they are, nonetheless, designed by human actors for use by, and in relation to, other human actors. The act of engendering trust involved in COVIDSafe implementation is consequently still an operation of trusting intention that is mediated through the legal and technical systems environment.

Importantly, the five dimensions of trusting intention identified by McKnight and colleagues are instructive to our consideration of the concepts of trust underpinning the COVIDSafe app implementation. These dimensions are, first, the risk of potential negative outcome. Several theorists, such as Deutsch, suggest "trust" is a "willingness to be vulnerable" to risk because trust has an inherent element of consequence associated with it.[90] If a trustor did not have their trust fulfilled, then the trustor, and, indeed, the trustee, would suffer. The absence of certainty in trust is much apparent in the COVIDSafe context. Uncertainty

[82] *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020* (Cth). See Greenleaf, "Australia's COVIDSafe App," 5–6.
[83] Taylor, "QR Codes."
[84] Greenleaf, "Phase III," 6.
[85] Bygrave, "Data Privacy Law."
[86] Burdon, "The Significance of Securing."
[87] Greenleaf, "Phase III"; Bell, "What Motivates People"; Leins, "Tracking"; Lodders, "Scrutinising COVIDSafe."
[88] McKnight, Meanings.
[89] Keymolen, "Negotiate," 240.
[90] Deutsch, "Trust."

about both the nature of the virus and the socio-economic effects of the pandemic, as well as the effectiveness of the COVIDSafe app, underscores the risk to the trustor and the trustor's vulnerability to potential negative effects arising from their trustworthy actions.

The second dimension of trusting intention is "dependence."[91] In the context of the COVIDSafe app and information privacy considerations, engendering trust in the public to achieve uptake requires the public's willingness to be dependent on the government to safeguard personal information. Dependence is tied to the third dimension of "feelings of security" that McKnight and colleagues identify as an emotional component against the other cognitive dimensions of trusting intention.[92] The fourth dimension is "situation specific" and underscores the previously mentioned point of the government's attempt at focused application of the COVIDSafe legislation, and restricted scope of use of personal information. The last dimension is a trustee's "lack of reliance on control" mechanisms.[93] This dimension of trusting intention separates the voluntary contact tracing app schemes from mandatory iterations that rely on power and control mechanisms rather than trusting the public to behave as desired.

However, we believe the focus on concepts of trust, even a more discrete focus on systems trust and its interplay with the dimensions of trusting intention, does not provide clear assistance in the trust-engendering implications of regulatory and rhetorical implementation strategies. The broader focus on concepts of trust only takes the critical discussion so far, and a more nuanced model that focuses on the trustee and examines signals of trustworthiness used to engender trusting intention and system trust is required. Therefore, we adopt the model of trustworthiness, proposed by Mayer and colleagues,[94] to examine regulatory and rhetorical actions ostensibly aimed at engendering trust in the COVIDSafe app.

Mayer observed three characteristics of trustee actions that can increase the level of trustworthiness perceived by trustors. These characteristic acts were conceptualized as ability, integrity, and benevolence to provide "a solid and parsimonious foundation" for the study of trust.[95] Trust results from an interaction between the "factors of perceived trustworthiness" exhibited by a trustee and the trustor's propensity to trust, based on those factors. Therefore, trustworthiness is conceptualized as the antecedent factors employed by a trustee that encourage the development of a trustworthy relationship with the trustor. Thus, trustworthiness fosters an "attitude that [the trustee] will help achieve an individual's [e.g., trustor's] goals in a situation characterized by uncertainty and vulnerability."[96]

The Mayer model of trustworthiness allows a closer examination of regulatory rationales and rhetorical campaigning from three different characteristic domains:

1. *Ability* connotes skill set and domain-specific competencies in a narrow technical area, or attributes that enable a trustee to "have influence" on the formation of trust.[97] In the context of COVIDSafe, ability is demonstrated through technical design and the domain-specific competencies and skill sets of both the app developers and policy implementers regarding the implementation of the app.
2. *Integrity* regards a trustee's governing principles that are aligned or considered in congruence with a trustor.[98] Integrity, in this paper, is defined as a form of "value congruence" where there is compatibility between trustee and trustor beliefs and values.[99] Regarding COVIDSafe implementation, we contend that integrity is demonstrated by willing trustee agreement to comply with information privacy law obligations, and societal expectations about the value of information privacy protections.
3. *Benevolence* entails the extent to which a trustee is believed to want to do "good" to the trustor[100]—or, at the very least, not to do harm. In the context of COVIDSafe, we consider this element demonstrated where a trustor forms the trusting belief that despite their information privacy concerns and risks to their own values of privacy, the deployment, take-up and continued use of the COVIDSafe app arise from a benevolent exercise of regulatory rationales and strategic rhetoric by public health authorities. In other words, signing up for COVIDSafe will lead to individual and societal goods, as the Australian Government does not intend to do harm from this act.

[91] McKnight, Meanings, 27.
[92] McKnight, Meanings, 8.
[93] McKnight, Meanings, 27.
[94] Mayer, "Integrative Model."
[95] Mayer, "Integrative Model," 717.
[96] Lee, "Trust in Automation," 50.
[97] Mayer, "Integrative Model," 717.
[98] Mayer, "Integrative Model," 720.
[99] Sitkin, "Explaining."
[100] Mayer, "Integrative Model," 718.

We use the Mayer framework to examine how trustor to trustee beliefs were employed in COVIDSafe implementation through the interplay of technical design as domain-specific *ability* competencies; the closer alignment of regulatory rationales and rhetorical campaigns as value congruent *integrity* strategies; and the open and transparent development of a *benevolent* value consensus to cement and support trustworthiness in the app.

Understanding COVIDSafe's Implementation Through Trustworthiness

We contend that a greater degree of regulatory and rhetorical alignment was required from the Australian Government to better signal trustworthiness to Australian citizens about downloading and using the COVIDSafe app. Greater alignment was possible when implementation activities were viewed from the lens of trustworthy-promoting actions that regarded ability, integrity and benevolence characteristics. We believe the central pillar of a COVIDSafe trustworthiness-promoting strategy had to be clearly benevolent in its overarching policy basis. A clear and signalled intention to "do good" should have guided regulatory rationales and rhetorical campaigning. Intention to do good would have involved an explicit attempt to seek an agreed value consensus about the app's use. Consensus should have then defined the value congruent actions of integrity through compliance with enhanced forms of information privacy law. It should then flow through to the specific ability competencies required for technical and legal implementation.[101]

Therefore, trustworthy alignment requires consistency of regulatory and rhetorical approaches across the domains of benevolence, integrity and ability. Alignment and consistency provide the basis for a coherent consensus seeking strategy that clearly signals the selfless intentions of the trustee, the Australian Government, that resonates with the values of the trustor, Australian citizens. It then indicates the specific requirements to be implemented that are redolent to ability considerations. However, as noted, some parts of the government's COVIDSafe implementation strategy were aligned but others were not.[102] We believe the misalignment occurred for two reasons.

First, there was an overt focus on processes of regulatory rationality that concentrated solely on the technical and legal protections of COVIDSafe. The protections highlight the ability and integrity considerations at play. Ability considerations focused on the technical capabilities of COVIDSafe, such as the limited types of data collected, particularly the design choice to collect Bluetooth data only, in combination with other technical protections, such as security and encryption of collected data. There was also a clearer alignment between how COVIDSafe operated technically and the integrity considerations involved in the enhancement of additional information privacy law protections. These enhancements provided additional legal guarantees to augment COVIDSafe's technical protections.

However, while there was alignment between the technical components of ability and the legal compliance requirements of integrity, the attempt at value congruence arising from both characteristics resulted in a predetermined assumption about trust. The assumption is, of course, the circular reinforcement highlighted at the start of this article, which equates the implementation of stronger information privacy law protections as resulting in the automatic acquisition of citizen trust. This paper highlights the frailties behind that assumption caused by the separation of ability and integrity considerations from benevolence characteristics. The congruence that integrity considerations seek to promote does not equate to the benevolent processes of trustworthiness based on genuine attempts at seeking value consensus.

In other words, the actions of seeking value consensus as benevolence and of displaying value congruence through legal compliance operate in two different ways to communicate trustworthiness. They are not the same actions and, thus, completing these two distinct acts without alignment does not necessarily equate to a trusted outcome. Key here is the circular reinforcement that naturally equivocates enhanced legal protections with enhanced trust. Our analysis would suggest that reinforcement as the sole way of engendering trust is misplaced. Consequently, an overt focus on regulatory rationality is, therefore, not a sufficient implementation strategy to enhance trustworthiness. Instead, it is also necessary to consider the important role of rhetorical campaigning as a benevolent signal that seeks to establish a genuine value consensus.

This leads to our second reason. The rhetorical campaigns adopted by the Australian Government were so wholly misguided that they were largely separate from the beneficial components derived from COVIDSafe technical and legal protections. There was a clear misalignment of regulatory and rhetorical implementation strategies.[103] However, more importantly, from a lens of trustworthiness, the rhetorical campaigns were not the type of value consensus seeking signal that benevolence characteristics require. The rhetorical campaigns had a prefabricated assumption about value consensus that was utterly misplaced. The assumption was that a discussion about value consensus was not required because downloading the COVIDSafe app was the

[101] Greenleaf, "Phase II," 4.
[102] Leins, "Tracking."
[103] Greenleaf, "Phase III," 38.

"right thing to do" from a wartime, "Team Australia" or an individual protection perspective. In other words, the Australian Government had not sought to determine or shape value consensus prior to imposing its own assumption of value upon Australian citizens. The implicit regulatory assumption that enhanced legal protections naturally engender trust, combined with the explicit rhetorical frame of moral compulsion, was the government's confused attempt at seeking value consensus from a benevolence perspective. It resulted in a strategy that basically stated that downloading the app was "entirely voluntary," but it had to be done, nonetheless.

We have noted the complex role of vulnerability and risk in establishing trust. Both the trustor and the trustee bear some degree of risk that requires them to be vulnerable to each other. Vulnerability is the shared component between trustors and trustees that engenders trust and provides the antecedence for trustworthy actions. The shared vulnerability of Australian citizens and the Australian Government at the time of the COVIDSafe roll out was palpable. It was a shared experience that gave rise to different risks, particularly in the information privacy law context.[104] There was a collective vulnerability that should have provided the basis for an open and genuine discussion about the need for value consensus and alignment with value congruence and competencies. However, instead of a mutual expression of vulnerability, the government's rhetorical campaigns provided a bludgeon of moral culpability. The effect of the bludgeon was so misplaced that it even detracted from promoting the value of the government's own vulnerability in implementing COVIDSafe. For a jurisdiction that is largely bereft of strong information privacy law protections, the implementation of COVIDSafe's legal guarantees were given at a policy cost that increases the risk of future public demand for stronger privacy law protections, and leaves the government vulnerable to prospective and unwanted policy changes in this sphere. A legal protection, once given, is much harder to then take away.

We contend that the government's claxon of moral compulsion drowned out the benevolent components of its own trustworthiness-inducing activities, demonstrated by the fact that there was only partial alignment between regulatory and rhetorical strategies. Moreover, there was a clear separation between the ability and integrity characteristics of regulatory rationality and the benevolence characteristic of rhetorical campaigning. The attempts at establishing trustworthiness in the implementation of the COVIDSafe app were consequently limited and misaligned. Instead, a much greater focus was required on the trustworthy characteristic of benevolence as a form of genuine value consensus seeking activity that should have then shaped the technical and legal characteristics of ability and integrity.

In our view, the attempts to genuinely seek a value consensus should have explicitly focused on the role of benevolence in establishing trustworthiness as the implementation strategy's core foundation. Central to the notion of benevolence is vulnerability. A benevolent and value consensus seeking approach would place much greater focus on an open and explicit acknowledgement of vulnerability by the Australian Government. To a certain extent, this acknowledgement did take place in the implementation strategy in the form of the "Team Australia" rhetorical campaigning. The basis of the campaign was that Australia, its citizens and its economy were all vulnerable to the health, economic and social risks posed by the pandemic. These risks were real given the substantial loss of life from transmission, the significant loss of jobs and the social disruptions caused by lockdowns. However, we contend that this sole expression of vulnerability would only assist so much to engender trustworthiness in a benevolent sense. Instead, the type of vulnerability required is akin to that noted above, where the trustor and the trustee are vulnerable to each other. In the information privacy context of regulatory rationality, we believe the signal of benevolence needed to be built on notions of fairness, and be constructed on transparent mechanisms articulating the process of value construction.

The focus on transparency in the formulation of value consensus contrasts with the rhetorical strategy that was built on moral compulsion. We contend that fairness propagates from Mayer and colleagues' integrity considerations, and acts as a signal to demonstrate alignment with shared values within the community. However, the shared values that underpin the conceptualization of fairness emerge from separate benevolence considerations. To demonstrate benevolence towards the trustor, a trustee must consider the contextual application of fairness, and the vulnerabilities that are accentuated from unfair dispositions, as part of a transparent value construction process. This transparent signalling of fairness, as part of an implementation strategy, becomes key to demonstrating benevolence in a trustworthy sense. However, the compulsion basis of the Australian Government's rhetorical campaign went against its own implementation strategy. The message of what was "right," what "Team Australia" was morally compelled to do, was disconnected from a construction of fairness required to demonstrate a benevolent intention. Instead, the message should have emerged from a benevolently driven articulation of values that attempted to capture citizen concerns, worries, pain and vulnerabilities.

Understandably, much of the moral compulsion that was built into the rhetorical strategy of COVIDSafe emerged from time pressures and the need to show a strong public response in the face of the pandemic. However, the approach was unsuccessful in achieving sufficient public trust to achieve the required uptake of the app, as the trustworthy element of benevolence could

[104] Greenleaf, "Phase III," 4.

not be fulfilled solely by a focus on legal instrumentality. We argue that an approach of transparent formulation of shared values would have ameliorated the narrative of moral compulsion, introduced proportionality into the policy decision-making process, and allowed the building of value consensus by explicitly breaking down information asymmetries inherent in governmental collections of personal information.

A benevolent approach would have reframed the original conceptualization of "protection" as moral compulsion that demanded an individual protect themselves and others, to "protection" as benevolent consideration of mutual vulnerability. We believe the Australian Government should have been more transparent about the imperfect inputs for policy and regulatory intervention, as well as the decision-making steps taken. It should have acknowledged its own exposure to risk arising from policy failure and the shared common vulnerability with the public. The need for greater transparency in respect of public health decisions was clearly highlighted by infectious disease experts who contended that decision-making at the policy level had been "too secretive."[105]

Similarly, the decision-making and communication by the Australian Government relating to vaccine supplies have generated similar criticism about the lack of transparency.[106] Critically, the failure to consider the shared vulnerabilities of state-based vaccination programs has led to uncertainty about second dose supply and the stockpiling of vaccines. Queensland Deputy Premier, Steven Miles, stated that transparency around dose supply was required to enable state governments to roll out their vaccination program effectively, and that communication about vaccine supply needed to be "transparent to the public, [and] transparent to… the media."[107] The Queensland Chief Health Officer, Dr Jeannette Young, also offered a clear example of how transparency of public health policy decision-making vulnerabilities could build public trust, despite leaning on wartime rhetoric.[108] Both considerations point to the fact that the choice of a compulsion-based notion of protection in the COVIDSafe implementation strategy was a conscious one by the Australian Government.

A shared position in vulnerability would have sent a different benevolent signal that was less oriented on paternalistic motivations to increase uptake of the tracing app, and away from the moral undertones that were ultimately unhelpful. Instead, we suggest transparent consensus building rather than moral compulsion would also drive new thinking about "proportionality," which has been conceptually thin in Australia. We see "proportionality" as a consideration of fairness that would find articulation in the benevolent exercise of value consensus formation. Thus, the relational acts in data collection and the appreciation of vulnerability in these acts would take precedence over rhetorical exercises serving purely to bolster uptake of the app. In effect, these are clear indicators as to why APP 3.5 considerations are important to ensure that compulsion as moral coercion is not perceived by the public as an unfair collection.

The disparity of regulatory and rhetorical approaches consequently provided an unclear benevolence signal in a trustworthy sense. This point is important because the role of benevolence could have provided a stronger signal of "good" intentions. In other words, an enhanced fairness perspective built on a transparent value consensus-building exercise would have provided a platform to develop a different type of rhetorical campaign that was not dependent on moral browbeating. Instead, it could have signalled benevolent intentions, such as the explicit enhancement of existing legal protections or as a basis for guaranteeing equitable treatment.[109]

Conclusion

This article examines the Australian Government's implementation of its contact tracing app, COVIDSafe. It demonstrates a misalignment between the regulatory rationale adopted and the rhetorical campaigning employed to engender citizen trust. The misalignment unfolds throughout the implementation strategy. The overall basis of the strategy regarded an overt focus on legal instrumentality combined with an emotive rhetorical campaign. At key points in the strategy, the emotive component was not in lockstep with the strategy's regulatory rationale. The strategy's focus sought to enhance the existing process protections of information privacy law, and rhetorical campaigning highlighted the broader relational consequences arising from COVIDSafe. Both elements focused on the same targets but in different ways, so there was a closer alignment in approach. The legal requirements needed to successfully implement the app, and to engender trust, necessitated new legislation to obviate the fragmented nature of Australia's information privacy law framework. However, while the new legislation ensured that the

[105] Layt, "Experts Call."
[106] Knaus, "Six Key Things."
[107] Lynch, "Queensland."
[108] Roberts, "Jeanette Young." Dr Young was quoted, "I think you've got to gain that trust in times of peace, so you can really go and use it in times of war."
[109] Lodders, "Scrutinising COVIDSafe," 159.

COVIDSafe collection was lawful, it opened the possibility that the rhetorical campaign was unfair, given the potentially coercive connotations that arise from the moral compulsion underpinning rhetorical campaigning.

This article also makes some important findings relating to trustworthiness. We adopted the Mayer framework and applied its three characteristic domains of trustworthy actions—ability, integrity and benevolence—that engender trust. In doing so, we further highlight misalignments within the implementation strategy, involving regulatory rationales and rhetorical campaigns, and highlight misalignments from a trustworthy perspective. We contend there was an overt focus on ability and integrity characteristics caused by the strategy's imperative of legal instrumentality. A further, and more important, misalignment occurred through the emotional focus of the rhetorical campaign. The campaign sought to foster trust derived through moral compulsion, because downloading the app was "the right thing to do." The assumption was predicated on legal instrumentality and the belief that enhanced legal protections would naturally lead to enhanced levels of citizen trust. That assumption, and its delivery through the rhetorical campaign, was misplaced, as evidenced by the low uptake numbers. Instead, a greater focus on the role of benevolence as a trust-intending signal of "doing good" was needed. The benevolent signal would have acted as an attempt to genuinely seek value consensus between the Australian Government and its citizens. Agreed consensus would have then created a clearer path on how to achieve value congruence through information privacy law, which could then have guided the legal and technical requirements of implementation.

This article suggests that novel governmental data collection systems, such as COVIDSafe, need to be clearly aligned from a trustworthy and implementation strategy perspective. These are important issues generally but specifically so regarding the ongoing COVID pandemic. As vaccine roll outs continue, and the focus of pandemic response shifts from lockdowns and transmissions to openings and health protections, then it is likely that the technological focus of pandemic response will move from contact tracing to vaccine passports. Many of the issues raised in this article will consequently have longer-standing considerations in pandemic response and beyond. It calls for a new way of achieving value consensus that goes beyond the limited conception of vulnerability exhibited by the Australian Government in its attempts to ensure uptake of the COVIDSafe app. In conclusion, we argue that a benevolently oriented COVIDSafe implementation strategy would have aligned the three domains of trustworthy actions in a consistent implementation delivery approach, thus, aligning regulatory rationality and rhetorical campaigning more conclusively.

Acknowledgements

The authors thank the two anonymous reviewers for their helpful and insightful comments.

Bibliography

Secondary Sources

Ahmed, Nadeem, Regio A. Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S. Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke and Sanjay K. Jha. "A Survey of COVID-19 Contact Tracing Apps." *IEEE Access* 8 (2020): 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226.

Alanzi, Turki. "A Review of Mobile Applications Available in the App and Google Play Stores Used During the COVID-19 Outbreak." *Journal of Multidisciplinary Healthcare* 14 (2021): 45–57. https://doi.org/10.2147/JMDH.S285014.

Australian Law Reform Commission. *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*. (Australian Law Reform Commission, 2008).

———. *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*. (Australian Law Reform Commission, 2014).

Bell, Genevieve, Mark Andrejevic, Christian Barry, Helen Christensen, Larissa Hjorth, Matthew Hornsey, Jolanda Jetten, Christopher Lawrence, Seth Lazar and Mark Taylor. *What Motivates People to Download and Continue to Use the COVIDSafe App?* (Office of the Chief Scientist, 2020).

Bennett Moses, Lyria and Anna Collyer. "COVIDSafe: Legal Issues." *Australian Law Journal* 94, no 7 (2020): 497–503.

Briefing. "Creating the Coronopticon: Countries Are Using Apps and Data Networks to Keep Tabs on the Pandemic." *The Economist*, 28 March, 2020. https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

Brinsden, Colin. "COVIDSafe App to Help Get Back to Normal." *Courier Mail*, 26 April, 2020. https://www.thecourier.com.au/story/6735355/covidsafe-app-to-help-get-back-to-normal/.

Burdon, Mark and Lizzie Coles-Kemp. "The Significance of Securing as a Critical Component of Information Security: An Australian Narrative." *Computers & Security* 87 (2019): 101601. https://doi.org/10.1016/j.cose.2019.101601.
Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.
———. *Data Protection Law: Approaching Its Rationale, Logic and Limits*. The Hague: Kluwer Law International, 2002.
Chee, Kenny and Tham Yeun-C. "S'pore Govt to Pass Law to Ensure TraceTogether Data Can Be Used Only for Serious Crimes." *Straits Times*, 8 January, 2021. https://www.straitstimes.com/singapore/legislation-to-be-passed-to-ensure-tracetogether-data-can-only-be-used-for-serious-crimes.
Clifford, Damian and Jef Ausloos. "Data Protection and the Role of Fairness." *Yearbook of European Law* 37, (2018): 130–187. https://doi.org/10.1093/yel/yey004.
Cohen, Julie E. "Turning Privacy Inside Out." *Theoretical Inquiries in Law* 20, no 1 (2019): 1–31.
———. "What Privacy Is For." *Harvard Law Review* 126, no 7 (2013): 1904–1933.
Couch, Danielle L., Priscilla Robinson and Paul A. Komesaroff. "COVID-19—Extending Surveillance and the Panopticon." *Journal of Bioethical Inquiry* 17 (2020): 809–814. https://doi.org/10.1007/s11673-020-10036-5.
Department of Health. "COVIDSafe: New App to Slow the Spread of the Coronavirus." Last modified 27 April, 2020. https://www.health.gov.au/ministers/the-hon-greg-hunt-mp/media/covidsafe-new-app-to-slow-the-spread-of-the-coronavirus.
Deutsch, Morton. "Trust and Suspicion." *Journal of Conflict Resolution* 2, no 4 (1958): 265–279. https://doi.org/10.1177/002200275800200401.
European Centre for Disease Prevention and Control. *Contact Tracing for COVID-19: Current Evidence, Options for Scale-up and an Assessment of Resources Needed*. (ECDC, April 2020).
Floreani, Samantha. "Navigating the COVIDSafe App Rhetoric." *Eureka Street* 30, no 10 (2020): 33–36.
Galloway, Kate. "The COVID Cyborg: Protecting Data Status." *Alternative Law Journal* 45, no 3 (2020): 162–167. https://doi.org/10.1177/1037969X20930431.
Goggin, Gerard. "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology." *Media International Australia* 177, no 1 (2020): 61–75. https://doi.org/10.1177/1329878X20949770.
Greenleaf, Graham. "Privacy in Australia." In *Global Privacy Protection: The First Generation*, edited by Graham W. Greenleaf and James B. Rule, 141–173. Cheltenham: Edward Elgar, 2008.
———. "'Tabula Rasa': Tens Reasons Why Australian Privacy Law Does Not Exist." *University of New South Wales Law Journal* 24, no 1 (2001): 262–269.
Greenleaf, Graham and Katharine Kemp. "Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law." *University of New South Wales Law Research Series* 40 (2020).
———. "Australia's COVIDSafe Experiment, Phase II: A Draft Law for Surveillance and Trust." *University of New South Wales Law Research Series* 33 (2020).
———. "Australia's COVIDSafe Experiment, Phase III: Legislation for Trust in Contact Tracing." *University of New South Wales Law Research Series* 24 (2020).
———. "Australia's 'COVIDSafe' Law for Contact Tracing: An Experiment in Surveillance and Trust." *International Data Privacy Law* (2021). https://doi.org/10.1093/idpl/ipab009.
Hayne, Jordan and Georgia Hitch. "Coronavirus App Will Not Be Forced Upon Australians, Scott Morrison Says." *ABC News*, 18 April, 2020. https://www.abc.net.au/news/2020-04-18/prime-minister-rules-out-making-coronavirus-app-mandatory/12161126.
Ivers, Louise C. and Daniel J. Weitzner. "Can Digital Contact Tracing Make up for Lost Time?". *The Lancet Public Health* 5, no 8 (2020): e417–e418. https://doi.org/10.1016/S2468-2667(20)30160-2.
Keymolen, Esther and Astrid Voorwinden. "Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm." *International Review of Law, Computers & Technology* 34, no 3 (2020): 233–253. https://doi.org/10.1080/13600869.2019.1588844.
Knuas, Christopher. "Six Key Things We Don't Know About Australia's Covid Vaccine Rollout Despite Promises of 'Transparency'." *The Guardian*, 7 April 2021. https://www.theguardian.com/australia-news/2021/apr/07/six-key-things-we-dont-know-about-australias-covid-vaccine-rollout-despite-promises-of-transparency.
Kretzschmar, Mirjam E., Ganna Rozhnova, Martin C. J. Bootsma, Michiel van Boven, Janneke H. H. M. van de Wijgert and Marc J. M. Bonten. "Impact of Delays on Effectiveness of Contact Tracing Strategies for COVID-19: A Modelling Study." *The Lancet Public Health* 5, no 8 (2020): e452–e459. https://doi.org/10.1016/S2468-2667(20)30157-2.
Landau, Susan. "Location Surveillance to Counter COVID-19: Efficacy Is What Matters." *Lawfare* (blog), 25 March, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters.
Layt, Stuart. "Experts Call for More Transparency Around Pandemic Decisions." *Brisbane Times*, 27 March, 2021. https://www.brisbanetimes.com.au/national/queensland/experts-call-for-more-transparency-around-pandemic-decisions-20210327-p57em3.html.
Lee, John D. and Katrina A. See. "Trust in Automation: Designing for Appropriate Reliance." *Human Factors* 46, no 1 (2004): 50–80. https://doi.org/10.1518/hfes.46.1.50_30392.

Leins, Kobi, Christopher Culnane and Benjamin I. P. Rubinstein. "Tracking, Tracing, Trust: Contemplating Mitigating the Impact of COVID-19 with Technological Interventions." *Medical Journal of Australia* 213, no 1 (2020): 6–8. https://doi.org/10.5694/mja2.50669.

Lodders, Adam and Jeannie Marie Paterson. "Scrutinising COVIDSafe: Frameworks for Evaluating Digital Contact Tracing Technologies." *Alternative Law Journal* 45, no 3 (2020): 153–161. https://doi.org/10.1177/1037969X20948262.

Lynch, Lydia, and Rachel Clun. "Queensland Will Supply Vaccine Faster if Supply is Made Public." *Brisbane Times*, 31 March 2021. https://www.brisbanetimes.com.au/politics/queensland/queensland-will-give-out-vaccine-faster-if-supply-is-made-public-20210331-p57fk0.html

Maddocks. *The COVIDSafe Application: Privacy Impact Assessment*. (Department of Health, April 2020).

Mayer, Roger C., James H. Davis and F. David Schoorman. "An Integrative Model of Organizational Trust." *Academy of Management Review* 20, no 3 (1995): 709–734. https://doi.org/10.2307/258792

McDonald, Sean. "The Digital Response to the Outbreak of COVID-19." *Centre for International Governance Innovation*, 30 March, 2020. https://www.cigionline.org/articles/digital-response-outbreak-covid-19

McKnight, D. Harrison and Norman L. Chervany. *The Meanings of Trust*. Minneapolis: Carlson School of Management, University of Minnesota, 1996.

Meade, Amanda. "Australian Coronavirus Contact Tracing App Voluntary and with 'No Hidden Agenda', Minister Says." *The Guardian*, 18 April, 2020. https://www.theguardian.com/technology/2020/apr/18/australian-coronavirus-contact-tracing-app-voluntary-and-with-no-hidden-agenda-minister-says.

Morley, Jessica, Josh Cowls, Mariarosaria Taddeo and Luciano Floridi. "Ethical Guidelines for COVID-19 Tracing Apps." *Nature* 582, no 7810 (2020): 29–31. https://doi.org/10.1038/d41586-020-01578-0.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books, 2010.

Office of the Australian Information Commissioner. *Australian Privacy Principles Guidelines:* Privacy Act 1988. (OAIC, 2014/2019).

———. "Privacy in Your State." Last modified 25 March, 2021. https://www.oaic.gov.au/privacy/privacy-in-your-state/.

Roberts, George. "Queensland's Jeannette Young Reveals There is No Rule Book in Dealing with a Once-in-a-lifetime Pandemic." *ABC News*, 21 March, 2021. https://www.abc.net.au/news/2021-03-21/qld-coronavirus-chief-health-officer-jeannette-young-conference/100018390.

Ryan, Mark. "In Defence of Digital Contact-Tracing: Human Rights, South Korea and COVID-19." *International Journal of Pervasive Computing and Communications* 16, no 4 (2020): 383–407. https://doi.org/10.1108/IJPCC-07-2020-0081.

"Scott Morrison Urges All Australians to Download COVIDSafe App, Says It's the 'Ticket' to Easing Restrictions." *SBS News*, 29 April, 2020. https://www.sbs.com.au/news/scott-morrison-urges-all-australians-to-download-covidsafe-app-says-it-s-the-ticket-to-easing-restrictions.

Sitkin, Sam B. and Nancy L. Roth. "Explaining the Limited Effectiveness of Legalistic 'Remedies' for Trust/Distrust." *Organization Science* 4, no 3 (1993): 345–512. https://doi.org/10.1287/orsc.4.3.367.

Smith, Paul. "Ministers Play Team Australia Card as Problems Undermine COVIDSafe App." *Australian Financial Review*, 4 May, 2020. https://www.afr.com/technology/ministers-play-team-australia-card-as-problems-undermine-covidsafe-app-20200503-p54pc0.

Taylor, Josh. "QR Codes: How an Old Technology Could Help Contact Tracers Keep the Pandemic in Check." *The Guardian*, 31 October, 2020. https://www.theguardian.com/world/2020/oct/31/qr-codes-how-an-old-technology-could-help-contact-tracers-keep-the-pandemic-in-check

Winer, Stuart. "Health Ministry Launches Phone App to Help Prevent Spread of Coronavirus." *The Times of Israel*, 23 March, 2020. https://www.timesofisrael.com/health-ministry-launches-phone-app-to-help-prevent-spread-of-coronavirus/.

World Health Organization. "WHO Director-General's Opening Remarks at the Media Briefing on COVID-19: 16 March 2020." Last modified 16 March, 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020

Worthington, Brett. "Chief Medical Officer Expects Staged Easing of Coronavirus Restrictions but Wants Physical Distancing Maintained." *ABC News*, 3 May, 2020. https://www.abc.net.au/news/2020-05-03/brendan-murphy-chief-medical-officer-coronavirus-update/12210198

Primary Sources

Cases

Griffiths v Rose [2011] FCA 30 (31 January 2011).

N and Law Firm [2011] AICRMN 8 (22 December 2011).

Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 (19 January 2017).

Legislation and Regulations

Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020 (Cth).
Explanatory Memorandum, *Privacy Amendment (Public Health Contact Information) Bill 2020* (Cth).
Privacy Act 1988 (Cth).
Privacy Amendment (Public Health Contact Information) Act 2020 (Cth).