Identifying and Mitigating Humanitarian Challenges to COVID-19 Contact Tracing

Kelsie Nabben and Paul Gardner-Stephen and Marta Poblet
College of Business and Law, RMIT University, Melbourne, Australia, kelsie.nabben@rmit.edu.au
College of Science & Engineering, Flinders University, Australia
Email: paul.gardner-stephen@flinders.edu.au
Graduate School of Business and Law, RMIT University, Australia
Email: marta.pobletbalcell@rmit.edu.au

2020 IEEE Global Humanitarian Technology Conference (GHTC) | 978-1-7281-7388-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/GHTC46280.2020.9342852

***Abstract*—COVID-19 contact tracing has rapidly emerged as a dynamic field of endeavor, with different countries taking different approaches, both politically and technologically. In this paper we examine the situation of Australia's development of a COVID-19 contact tracing application (which is in reality a proximity tracing application) as a case-study. Both technological and societal elements are considered, in particular, the delivery of poor protection, or the perception of poor protection, of privacy and civil liberties to negatively impact the adoption of such an application, and thus hamper its potential.**

The rest of the paper explores this digital-politic nexus and tensions within crisis response, and examines the trade-off can be improved through increasing public trust of such technologies by improving their actual and perceived privacy and human rights properties without reducing their medical effectiveness. Lessons for humanitarian organizations are extracted from this.

I. Introduction

A wave of government issued technology responses are being implemented globally in response to the COVID-19 pandemic. Around the world, governments have leaped at the opportunity to implement technical responses in the form of facial recognition cameras [1], surveillance drones [2], digital currency welfare pay-outs [3], artificial intelligence [4], and digital public health rating systems, as used in China [5].

While public-health and safety amid crisis is imperative, the data rights and privacy policy responses that occur at this critical juncture, and afterwards, must be carefully considered, because they directly influence the adoption and effectiveness of these technologies to reduce the pandemic's human cost.

A. *Contributions*

The key contributions of this paper are:

1) A snap-shot of the COVID19 contact-tracing mobile application trends around the world, viewed as an acceleration of pervasive government and corporate surveillance.
2) A case-study on the evolution of Australia's COVID-19 contact tracing app.
3) Evidence that protecting privacy and other human-rights is important for the effectiveness of humanitarian interventions that necessarily impinge on civil liberties, privacy and other human-rights.
4) Possible policy responses and technical attributes to improve digital-political responses to crisis and reflections on lessons learned for the humanitarian

B. *Structure of this paper*

The remainder of this paper briefly reports on global digital-political responses to COVID-19 (Section II), with a particular focus on Australia's evolving response (Section III) and COVIDSafe tracking application (Section IV), before moving on to discuss privacy concerns and their impacts on humanitarian interventions (Section V), an exploration of what could be done to improve the situation (Section VI), and surfacing lessons from this crisis for humanitarian responders and organizations (Section VII).

II. Importance of Digital-Political Responses

As COVID-19 has spread, so have smartphone-based contact-tracing applications. Countries that already leverage Bluetooth or GPS based tracking apps include China, Singapore, Israel, South Korea, Czech Republic, Poland, Macedonia and Ghana [6]. Some have taken a centralized approach to digital contact tracing, by integrating back-door data sharing capabilities within popular e-commerce or chat apps. For example, the Chinese Government worked with native 'super app' providers Alipay and WeChat to roll out a pseudo-optional, pervasive approach to data sharing [7]. Others have attempted to minimize government access to, or responsibility for, user data and have offered opt-in applications, like that of Singapore's TraceTogether [8].

Various nations that are still designing and considering an app-based response include Germany, the European Union, the UK [9], Russia [10], New Zealand and Australia [11].

In the European Union, there is not yet consensus on whether to use centralized or decentralized approaches to contact tracing. For example, Germany initially backed the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) [12], a centralized, GDPR (General Data Protection Regulation) compliant, standard to support international interoperability while deploying contact tracing solutions at the local level. Following criticism from the scientific community and refusal by Apple to facilitate centralized collection methods, the German government reversed its decision to support a decentralized solution [13], while other European states, such as France or the UK, still back the centralized approach [12].

Despite these conflicting approaches on how to best trace and store epidemiological data, there is also political interest in how these apps can inter-operate to create a global database of phone generated tracing data [14], [15].

The centralized approach impinges more on the privacy and civil liberties of citizens than a decentralized approach, that avoids the creation of any large data-set that describes the social or other interactions of people. This can result in diminished trust, adoption, and compliance, which can in turn affect the contact tracing effectiveness, as most of a population is required to participate for them to be effective [16]. Furthermore, a decentralized approach reduces the risks associated with holding and protecting this sensitive data.

The reason most people are required to use a contact tracing app for it to be effective is mathematical: If p is the proportion of the population use the app, then the chance of any given transmission being detected is n^2. If $n = 0.12$, the proportion of the Australian population using the app at the time of writing, then only $n^2 = 0.0144$, i.e., about 1.4% of transmissions will be detected. Even at the government's target of 40%, this still results in a detection rate of only 20%. To raise the detection rate to just 50%, 71% must run the app.

Therefore every aspect of such an contact tracing system must be carefully handled, so as to avoid creating opportunity for mistrust or mis-use, whether the digital system itself, or the political messaging and actions surrounding it. In the following section, we examine Australia's response, and where opportunities for further minimizing these effects might exist.

III. Australia's Digital-Political Response to COVID-19

Australia's digital-political response to the COVID-19 pandemic has evolved over time. Three key stages so far are as follows: (1) Public messaging and release of a COVID-19 informational app that does not do contact tracing [17]; (2) Access of mobile phone location data under existing laws to verify social distancing [18]; and (3) Public messaging and release of a COVID-19 contact tracing app [19]–[21]:

A. COVID-19 Informational App

At the end of March, the Australian government released an informational app, i.e., not contact tracing, built as an extension of Facebook owned 'Whatsapp'. The goal of this was to help Australians "Stay up to date with official information and advice about the corona virus ... situation." This app is not particularly contentious, and is mostly mentioned only to avoid confusion with the second app, which does contact tracing.

That said, it does have an important role to play in providing the public with up-to-date information on the COVID-19 situation in Australia, and Australia's policy settings on that. In this regard, it is a helpful communications tool.

B. Accessing Mobile Phone Data to Verify Social Distancing

Existing legislation that allows Australian authorities to access mobile phone data for law enforcement purposes is already in place. This has been used to gain data about the degree of adherence to social distancing [18]. It is also possible that it has been used to verify self-quarantining. However, the secrecy provisions of the request mechanisms mean that the mobile network providers are not able to confirm if they have had any such requests made to them, although, they have 'complied' with requests from the government [18].

Indeed, it is the lack of transparency in this situation that has created caution and distrust. Or rather, it is the repeated theme of the opacity of surveillance that seems to be the key problem of digital crisis responses, and one that feeds into the third element in significant ways.

C. Lead-up to, and Introduction of COVIDSafe App

The introduction of a contact tracing app in Australia was anticipated for two weeks, with the government announcing its intention to introduce an app, which was subsequently made available in late April [22].

This was preceded by considerable announcements regarding what the app would, and would not do, and whether it would be mandatory to use it. The Australian government are seeking an adoption rate of 40% or higher. Early statements indicated that there was consideration of making its use mandatory [16], and that it might track user's location, before being forced to explicitly exclude those policies [23]. These early missteps, together with issues relating to the collected data being under the control of a foreign cloud-server provider stimulated the Australian public's collective memory of mission-creep in surveillance in Australia. [24].

For example, using mobile phone meta-data to prosecute illegal sign posters [25], when the initial provision was created to address terrorism. In total, the Australian Federal Police accessed phone and/or internet meta-data more than 20,000 times in one year – including that of journalists, as they investigated the source of a story that embarrassed the government [26]. This investigation escalated to the raid of a journalists home, which the Australian High Court found to be unlawful [27].

Together with residual concern about the security of data held by the government [28], there is considerable hesitance among Australian commentators, industry experts and academics to install the contact tracing app [29], [30], even as government officials explain that restrictions could be relaxed sooner if the app is adopted more broadly [31], [32].

IV. Australia's COVID-19 Contact Tracing App

The Australian Government's COVID-19 contact tracing app, COVIDSafe, is based on Singapore's TraceTogether app. TraceTogether works through Bluetooth (RSSI) based mobile phone contact-tracing [33]. The application itself is opt-in and not compulsory to access any other public services.

Users set a PIN locally in the app. The Ministry of Health collects the mobile phone number of participants as well as a randomly generated UserID, which is cryptographically hashed. Proximity data is collected in a peer-to-peer fashion via Bluetooth, when a user comes within signal range of another phone that has the application. Public announcements say the application uses a decentralized approach to data management as all users' data are stored locally on the user's device and deleted after 21 days, or, if diagnosed with COVID-19, are uploaded to a centralized, third-party Amazon web-server cloud database [24]. Early analysis indicates that app mostly does what it claims, and is well built [19].

If diagnosed, a user can voluntarily share their proximity data with the Ministry of Health by disclosing the locally generated PIN. The Ministry of Health manages the private key to decrypt the UserID and access the contact-tracing data logs. The data is then used to by the Ministry of Health to contact people that have been in proximity with those affected for faster tracing and diagnosis.

Data is claimed to be exchanged between phones after 10 – 15 minutes of being in contact, the length of interaction which most people should be able to recall over the last fourteen days, as with traditional contact tracing interviews. Although examination of the app has revealed that it exchanges and retains data immediately, without first waiting for the 10 – 15 minute contact period [19], despite the government's statements to the contrary. This is an obvious by-product of the Bluetooth signal, which continually picks up as much proximity data as possible [34]. This has fuelled resistance to the application among the Australian public. Full specifications and source-code for the app are still to be released, although the government has promised to do so.

While there are sensible technical and legal reasons for these behaviors, the contradictory messaging that has resulted does not help to increase confidence in the app by the Australian public. Communications in crisis must be clear and decisive. Contradictions increase the likelihood of citizens being more critical of the privacy intrusions of digital interventions, either necessarily as intrinsic to contact tracing, or as conscious design decisions by the government, such as the choice to mandatorily record postcode and telephone number.

V. Privacy Concerns

There has been a diversity of responses from the Australian public to the privacy issues raised by the COVID-19 pandemic. Already, some 3 million Australians have downloaded and installed the app in its first week, and 1 million on the first day, indicating at least tacit approval of the trade-off of privacy and related civil liberties. Whether adoption will continue to grow at this rate, or whether the existing installations represent the majority of those willing to install it, remains to be seen. However, it is clear that conceptions of what are necessary, proportionate and appropriate privacy measures differ between the government and the public.

One response of populations observed by the authors in crisis scenarios when it comes to government surveillance and information collection at scale is "I've got nothing to hide" [35].

Yet, the fallacy of the "nothing to hide" argument is that privacy is not stolen in a single, one-directional attack. Privacy is a layered construct. It is a principle embedded (built) into technical, legal, moral, economic and societal layers of norms, and it also shapes these norms. This means that privacy is won or lost incrementally. It is the mass aggregation, social network mapping, data mining, secondary use and de-anonymization after collection that may potentially erode human dignity and both digital and social rights.

COVID-19 has been coined the new War On Terror, with mass compliance to changes in data rights and privacy encouraged in the interests of public health and, ultimately, national security, similar to that seen post the September 11 terrorist attacks [36]. At the same time, COVID-19 is also inaugurating a new era of global pandemic surveillance with ripple effects at the societal level that are yet to be fully understood.

The problem with government issued applications designed in conjunction with closed, proprietary interests is that citizens have little say over the scope of data collection about them or "the development of private platforms, run by private entities, with often opaque decision-making processes, behavioral analytics and identity profiling and data on-selling" [37]. The design, implementation and use of complex socio-technical systems must be driven be the interests of users [38].

Privacy, both as a principle and as a human right, is the responsibility of everyone. "Most Australians are concerned about their privacy online and are concerned about privacy violations by corporations" [37]. As a structural problem, privacy can be addressed through both top-down policy measures, as well as bottom-up technology features to still achieve the necessary aims of contact reporting, public health and safety.

A better response by government, could be to openly share contact tracing requirements, and allow industry and the open-source community to discover innovative solutions, with varying degrees of respect for privacy. As long as solutions were interoperable, people could choose according to their level of comfort and cooperate with government to own the crisis response.

A. Setting Privacy Precedence: The Privacy of the Singapore App

While the Singapore's TraceTogether app design purportedly blends considerations for individual data privacy preservation with centralized crisis response for efficiency, it is not clear how privacy-friendly it is from a user perspective. The application collects anonymized data about the user's device, such as phone model [39]. Furthermore, the Temporary ID's exchanged between phones via Bluetooth is generated by encrypting the User ID with a private key held by the Ministry [40].

Although the privacy statement of TraceTogether is more privacy aware than most proprietary applications that smartphone users accept daily, the full source code and documentation is not available for others to audit the code base [8].

Users can request that their data be revoked from storage, however, this requires further data sharing in the form of an email address and a level of trust that data will actually be permanently expunged.

Adopting the Singapore app approach in Australia has both advantages and drawbacks to be considered. What people find acceptable as a level of privacy in one context, such as was acceptable for 20% of Singapore's population at the peak of the crisis, may not apply to another environment, such as Australia's largely contained COVID-19 curve [41]. This is particularly relevant if tracing data is linked internationally across jurisdictions and expanded for other purposes, such as travel immunity passports.

B. Privacy Concerns with the Australian App

While acknowledging the importance of public health, the breadth and depth of privacy concerns arising from mobile phone-based contact-tracing cannot be downplayed.

The Australian Government finally launched its opt-in phone application on April 26, 2020, aiming for 40% adoption [31]. Less than 48 hours later, 2.5 million Australians are reported to have downloaded the app, while app related hoax text messages started to circulate [42]. Given the burden of responsibility on Governments to manage a centralized database of critical information on their population against hacks from malicious third-parties, localized proximity data storage on users' phones until diagnosis and warning of others is a wise approach [43].

Authorities in Australia have previously been criticized for working with telecommunication providers to access personal phone data and enforce mandatory home isolations without announcement or permission [25], [27], [44]. This level of digital surveillance is also prolific in China and the USA.

In times of crisis, governments trend towards expansive, top-down, centralizing measures because they are convenient and clear to administer [45]. However, they present challenges to privacy and democratic freedoms and accountability. The populace tends to recognize this implicitly: that governments do what is convenient for themselves above what the public perceives as being in the public interest. Importantly, this is independent of what intervention is actually being proposed. If a government gives unclear messaging in an unfolding situation when there is perhaps not a complete understanding of the implications of what is being proposed, in a rapidly evolving policy area, then the public will tend to suspect the worst. It is critical to limit the protracted nature of this tension in a crisis. As seen in Australia with the time and attention given to developing and explaining a contact tracing app, efficiency is not always achieved by resorting to the centralized, authoritarian model for the sake of efficiency.

This seems to be the case in the Australian COVID-19 tracking app context as the tension played out between how the app should be designed and administered. The first stratum of this debate is whether the app should be mandatory or voluntary, with the Prime Minister and the Deputy Chief Medical Officer not ruling it out and the Prime Minister saying it would not be compulsory but encouraging Australians to do their 'national service' [16]. The second stratum is whether the app is able to trace people's location, with the Minister for Government Services promising 'There is no geolocation, there is no surveillance, there is no tracking'. Thirdly, the app was claimed to be based on the Singapore's only recently open-sourced TraceTogether design, but the Government would be publishing the source code [20].

The Australian research and cryptography community have actively engaged in analyzing what is known about the TraceTogether application to escalate concerns and suggest improvements for a more decentralized, privacy-preserving approach [46]. In the current community anxiety about the use and misuse of data, the Australian Government has been forced to acknowledge it will be difficult getting people to download an ambiguous app [29].

Following multiple Government clarifications, it appeared the app will use the more private model, whereby data stays on the phone under user control until infection is confirmed, rather than the model which collates all contact data from all Australians and creates a pervasive surveillance database. Yet this has not been the case as the situation has unfolded.

The conflicting messaging surrounding privacy from the Australian government during the development of the COVID-19 tracing app continued with the announcement that the contract for the online services, presumably including the database, had been awarded to Amazon [24]. This is significant, because: (1) It means that a foreign controlled entity will be in control of highly sensitive data about Australians; (2) It provides an end-run for Australian law enforcement and secret services to access the data via the Five Eye's intelligence sharing mechanism, because any law prohibiting Australian distribution of the database would not apply to the USA's intelligence community, who would be able to use their legal powers to compel Amazon to divulge the data, from where it could be freely handed over to their Australian liaisons. Thus, apart from the self-evident reality that information critical to national security, which COVID-19 has shown must extend over public health data, should not be dependent on foreign entities or government, precisely because it is globalized supply chains that have been hit hardest.

Whether they were planning the former or the latter from the outset is difficult to tell, noting that the app or the code has not yet been released at the time of writing. What is clear is that the lack of transparency during the early stage of the process left room enough for Australians to quite reasonably jump to conclusions at the worst-case scenario end of the possible solution space the government might be considering.

C. Privacy Concerns Go Global

The TraceTogether development team is encouraging interoperability with similar applications, meaning that the data of Australian citizens could potentially feed into an international tracing database. The World Health Organization (WHO) is also advocating for interoperability between contact tracing apps [47]. The European Union has begun working on an EU Bluetooth based phone tracking application for the entire continent. With the emergence of a vernacular of 'disease surveillance', concerns with a global database are linked to access, control and many of the broader discrimination concerns of digitally linking multiple sources of identification data [48].

The WHO is also developing specifications for their application, including localization into many lanuages [49]. It is not yet clear whether this will simply be an informational app, or would participate in national contact tracing systems, although UI mock-ups suggest the former.

The EU has similarly proposed an anonymized and aggregated data pool by June 2020 for modeling, prediction and containment, including confinement [50]. De-anonymizing social network data has been possible for over a decade [51]. Furthermore, de-anonymization powers being afforded to Ministers are being considered in some jurisdictions [52].

Contact-tracing apps will require API changes from both Apple and Google to be most effective. This has contributed to an unprecedented partnership between Apple and Google for deployment of the world's largest population monitoring capabilities for the sake of contact-tracing [53]. The stated aim of these corporates is to integrate contact-tracing into the operating system layer, meaning that the closed, proprietary settings of the technology are not optional.

The convergence between private, profit-driven technology companies and government issued digital solutions in crisis is fraught with risk. The Australian Competition and Consumer Commission (ACCC) is currently suing Google for misleading Android users about location data and is reportedly worried about the "market power" of centralized platform providers [54]. These misleading screen prompts are known as dark technology patterns, designed to coerce user behavior not to their advantage [55]. Despite the ACCC case against Google, Australian law enforcement and security agencies can already access the meta-data on everyone's phone calls, text messages and emails [56]. Contact-tracing apps increase these hazards.

Both individual data privacy preservation and centralized crisis response for efficiency are necessary. However, with Australian COVID-19 cases under reasonable control, there is time to construct and iterate on a carefully considered digital-political response. A number of alternative policy and technical approaches can be considered to address the actual problem of virus tracing for faster reporting and testing.

VI. What Can Be Done?

There are a number of possibilities for enacting positive change in this area, so that both human rights, including privacy and civil liberties, and the public health objectives of digital contact tracing, can be better met. One framework to evaluate digital technologies in society is in terms of code, markets, laws and norms [57]. By analogy, we consider policy pathways and obfuscation (laws and norms), technology design approaches and cryptography (code) and hardware (markets).

A. Policy Pathways

If we believe in trust, democracy and the political process, then some of these concerns with the Australian Government's smartphone contact-tracing application can be addressed with proper due diligence in an open consultation process.

Pleas for careful consideration of COVID-19 related surveillance measures are taking place in the US, with a number of open letters calling for respect for human rights through:

- Only lawful, necessary and proportionate surveillance
- Temporary, time-limited powers with clear sunset clauses
- Data collection and aggregation only used for responding to the COVID-19 pandemic
- Government responsibility for sufficient cyber-security
- Addressing discrimination in the use of tools like big data analytics and machine learning algorithms
- Transparency, including legally binding and publicly shared data sharing agreements, where applicable
- Effective remedies for accountability against abuse and timely information sharing of any changes in terms
- Free, active and meaningful stakeholder participation [58]
- Open-sourcing all elements of the system, so that backdoors and faults can be identified and corrected, and also to allow concerned parties to build their own versions of the applications, rather than having to trust a third party to not modify the source code before compilation.

The EU's app development consortium promises a privacy preserving app that adopts some of the Singapore approach, but with a heavy emphasis on GDPR compliance and an open call to technology and design communities for input [14].

The European Commission has compiled a detailed list of virus app policy considerations. EU Member States are converging towards effective app solutions that minimize the processing of personal data and recognize that interoperability between these apps can support public health authorities and support the reopening of the EU's internal borders. The proposed approach is stated to be voluntary, approved by the national health authority, privacy-preserving and dismantled when no longer needed [50]. These policy approaches require trust in government and due democratic process.

It is imperative to interrogate design approaches and options as well, given the necessarily reactive nature of political-digital responses in crisis, the complex interests of numerous public and private stakeholders involved and what is at stake for populations around the world.

Protecting public health over privacy is a false dichotomy. This is where the opportunity for governments to do digital responses well, by advocating for trust-less digital infrastructure that supports a healthy, robust democracy. Trustlessness, the need to not rely on technology, government or businesses to safely handle data, can be in-built through cryptographic mechanisms and design to help protect end user privacy and more effectively aid public-health through increased adoption due to the trustability of digital guarantees over legal ones.

For trust-less (or trust enhancing) digital infrastructure, both cyber and physical elements of digital infrastructure must be considered [59]. That is, not only does the software elements need to be robust and trustworthy, such as the COVID-19 app, but also the devices that it runs on, i.e., mobile smartphones, and the up-stream infrastructure on which they depend, such as cellular networks and cloud-based service infrastructure.

B. Technology Design Approaches

Contact-tracing technology is not a new area of research, yet, previous scientific approaches have not been heavily referenced in the rush to design brand new phone apps [60]. Privacy researchers have warned the app needs to be more decentralized, so that the central servers that store the IDs do not become honeypots for potential hackers [46]. The centralized servers of multilateral organizations have been a target of successful hacks in recent history [61].

For example, even if the app is secure and privacy respecting and able to be audited, it must still run on proprietary smartphones that are not trustable from the end-user perspective. Aside from security vulnerabilities, laws like the Assisted Access Act in Australia mean that government can access any and all data on a smart-phone [62]. For end-users, the security of their data is based on promises and actual behavior of the government and its agencies, rather than on physical trustability of the digital infrastructure that they are using.

A number of well-respected industry individuals, groups and companies from around the world have openly published contact-tracing app guidelines, including CCC [63] and the TCN Coalition of privacy-first advocates, who have published Data Rights for Digital Contact Tracing and Alerting [64].

A technical response must consider the integration of these design features and especially not be linked to a person's phone or other personal identifiers. This includes cryptographic primitives, hardware and obfuscations.

C. *Cryptography — Trust in Maths*

The basic principles of a technology-based traceability response could also be informed by cryptographically secure, decentralized design principles. The origins of blockchain data sets are based on the tenants of decentralization of data and privacy. The fundamental mechanisms that could be considered include cryptographic primitives; such as homomorphic encryption and zero-knowledge proofs (that cryptographically prove information without revealing personal data) [65].

MIT's Private Kit: Safe Paths team has released the code base for a Privacy-by-Design COVID-19 GPS and Bluetooth tracing app [66]. They are reportedly planning another iteration of the solution with safer server hashing by having a hashing server and a storage server, controlled by two different organizations to avoid hash-cracking [67]. A team at McGill University have proposed the use of mix networks, to route hashed location trails through multiple servers to obfuscate the location and time-stamps from any particular user [68].

D. *Hardware — Smarter than a Smartphone*

Contact-tracing can also be addressed with hardware, by foregoing the assumption that the technical solution must be mobile phone based. One such example of an alternative hardware design being supported by the NLnet Foundation is Simmel [69]. The design is a pen-like device (Figure 1), which is a wearable hardware beacon and for Bluetooth based or NUS ultrasound frequency contact tracing, that can be handed in to health experts if diagnosed. Simmel is a viable approach to safely de-link personal data identification points, while achieving public health objectives for contact tracing.

E. *Obfuscation — Method in the Madness*

Obfuscation is the method of evasion, protest and sabotage against digital surveillance by deploying more data, rather than less [70]. One such method is differential privacy. Differential privacy is a method of injecting precise amounts of statistical noise into results drawn from data-sets, to protect individuals from being identified in aggregated data with mathematical guarantees of privacy. Differential privacy has been proposed by the Open Technology Institute in the US [71].

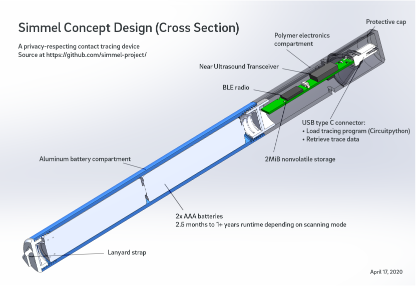
Simmel Concept Design (Cross Section)
A privacy-respecting contact tracing device
Source at https://github.com/simmel-project/
Protective cap
Polymer electronics compartment
Near Ultrasound Transceiver
BLE radio
USB type C connector:
• Load tracing program (Circuitpython)
• Retrieve trace data
2MiB nonvolatile storage
Aluminum battery compartment
2x AAA batteries
2.5 months to 1+ years runtime depending on scanning mode
Lanyard strap
April 17, 2020

Fig. 1. Simmel is a small disposable hardware device the can perform contact tracing alone. Being single-purpose, and transparent in design and operation it is designed to help user's protect their privacy, and engage with contact tracing without unnecessary fear of mis-use of their data. Image copyright Bunnie Huang. Apache License v2.

These examples and the efforts of teams around the world demonstrates that there are better approaches to contact-tracing. Adopting privacy- oriented design principles can greatly benefit and protect the public sector and public policy makers from the risks associated with database management and geopolitical targeting. Governments can leverage this opportunity to increase adoption and protect their constituents avoiding data convergence and keeping data points separate, including phone number, location data, digital identity, digital currency and digital health records, and support industry experts to develop best practice digital public health interventions.

The success of smartphone traceability apps to improve reporting and testing will also depend on norms of how the apps are used in society [72]. Technology solutions to a people-based problem frequently have unintended consequences.

VII. Lessons For Humanitarian Organizations

The contact-tracing app debate highlights some important lessons for humanitarian response groups regarding the role, design, deployment and communications of crisis response technologies. These issues touch on the challenge of capability maintenance in a complex and hostile cyber environment.

The effort required for humanitarian responders and agencies to select, vet and operationalize physical digital infrastructure, such as smart-phones, is considerable. Such devices become rapidly outdated and receive non-transparent software updates.

Meanwhile, installing software updates invalidates any prior security analysis, because the software domain has mutated. This amplifies the amount of work required to maintain such capabilities, and together with the previously discussed problems of legal back-door access to devices from potentially multiple jurisdictions, makes almost any modern digital device rationally untrustable [73]. This is why initiatives that can create long-term sustainable digital infrastructure and capabilities are critical to ensuring the mission of humanitarian endeavors.

These issues are not limited to contact tracing, but are of relevance to the general use of smart-phones and computers in humanitarian contexts.

Unfortunately, digital communications infrastructure is viewed as a subordinate element by most humanitarian aid organizations, despite being fundamental to crisis response efficiency, as demonstrated during COVID and numerous other cases of crisis response. Communications infrastructure is rarely tackled in a systemic and strategic manner with sufficient resources, to identify and create long-term, pre-emptive solutions. Relying on commercial, off-the-shelf products is not a solution to this problem, as it delegates trust to the commercial vendors, and does not in any way mitigate the long-term capability security maintenance or trust issues.

VIII. Conclusion and Future Directions

During any crisis, political and digital responses are complex. Australia's (and many other nations) political-digital COVID-19 response demands continued attention and iterative improvement. As useful as these tools are for public health, they could easily be misused post-crisis to intrusively manage the public's health, identity, wealth and movement and create precedence for this scale of response in other crises.

Passing of crisis legislation and imposing digital monitoring mechanisms surfaces tensions between the digital lives of entire populations and civil liberties and the trade- offs that need to be considered in the design and integration of digital tools.

Greater collaboration is required by both researchers and practitioners in the humanitarian fields of endeavor. On the one hand, solutions that respect privacy and human rights need to continue to be developed by industry experts in readiness, according to the human rights principles of transparent, temporary and proportionate. On the other hand, humanitarian practitioners need to continue to advocate for, and where possible influence in favor of deployment of such technologies.

References

[1] M. Ricks and L. Menand, "Coronavirus outbreak is major test for russia's facial recognition network," 2020. [Online]. Available: https://www.themoscowtimes.com/2020/03/25/coronavirus-outbreak-is-major-test-for-russias-facial-recognition-network-a69736

[2] M. Richardson, "'pandemic drones': Useful for enforcing social distancing, or for creating a police state?" 2020. [Online]. Available: https://theconversation.com/pandemic-drones-useful-for-enforcing-social-distancing-or-for-creating-a-police-state-134667

[3] M. Ricks and L. Menand, "Coronavirus stimulus: Let's pay it in digital dollars," 2020. [Online]. Available: https://www.bloomberg.com/opinion/articles/2020-03-24/coronavirus-stimulus-let-s-pay-it-in-digital-dollars

[4] A. Engler, "A guide to healthy skepticism of artificial intelligence and coronavirus," 2020. [Online]. Available: https://www.brookings.edu/research/a-guide-to-healthy-skepticism-of-artificial-intelligence-and-coronavirus/

[5] P. Mozur and R. Zhong, "In coronavirus fight, china gives citizens a color code, with red flags," 2020. [Online]. Available: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

[6] F. Bajak and N. Winfield, "Europe eyes smartphone location data to stem virus spread." 2020. [Online]. Available: https://www.usnews.com/news/us/articles/2020-03-23/europe-eyes-smartphone-location-data-to-stem-virus-spread

[7] I. Metha, "China's coronavirus detection app is reportedly sharing citizen data with police." 2020. [Online]. Available: https://thenextweb.com/china/2020/03/03/chinas-covid-19-app-reportedly-color-codes-people-and-shares-data-with-cops/

[8] G. of Singapore, "Trace together," 2020. [Online]. Available: https://www.tracetogether.gov.sg/

[9] M. Hancock and R. Mason, "Uk app to track coronavirus spread to be launched," 2020. [Online]. Available: https://www.theguardian.com/politics/2020/apr/12/uk-app-to-track-coronavirus-spread-to-be-launched

[10] L. Kelion, "Moscow coronavirus app raises privacy concerns," 2020. [Online]. Available: https://www.bbc.com/news/technology-52121264

[11] S. Kilgallon, "Coronavirus: Kiwi tech firm offers up covid-19 app to government," 2020. [Online]. Available: https://www.stuff.co.nz/technology/apps/120918665/coronavirus-kiwi-tech-firm-offers-up-covid19-app-to-government

[12] "Pan-european privacy-preserving proximity tracing," 2020. [Online]. Available: https://www.pepp-pt.org/

[13] D. Busvine and A. Rinke, "Germany flips to apple-google approach on smartphone contact tracing," 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J

[14] "Decentralized privacy-preserving proximity tracing," 2020. [Online]. Available: https://github.com/DP-3T/documents

[15] "Covid-19 - who app synthesis (for review) - google dokument." 2020. [Online]. Available: https://docs.google.com/document/d/1isNMLpwI2iUY92KPwJHfY7kQnpN3oCuUl6c94J7Qmhs/edit

[16] "Deputy chief medical officer doesn't rule out forcing australians to download thegovernment's coronavirus tracing app," 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-17/paul-kelly-coronavirus-tracing-app/12158854

[17] "Coronavirus australia app," 2020. [Online]. Available: https://www.health.gov.au/resources/apps-and-tools/coronavirus-australia-app

[18] I. Lane, "Privacy fears as governments use phone data to track coronavirus rule-breakers," 2020. [Online]. Available: https://thenewdaily.com.au/life/tech/2020/04/06/coronavirus-phone-location-tracking-data/

[19] B. Alsinglawi, M. Elkhodr, and O. Mubin, "The governments coronavirus mobile app is a solid effort, but it could do even better," 2020. [Online]. Available: http://theconversation.com/the-governments-coronavirus-mobile-app-is-a-solid-effort-but-it-could-do-even-better-135030

[20] J. Taylor, "Australia's coronavirus contact tracing app: What we know so far," 2020. [Online]. Available: https://www.theguardian.com/world/2020/apr/17/australias-coronavirus-contact-tracing-app-what-we-know-so-far

[21] M. Farr and D. Hurst, "Australian government plans to bring in mobile phone app to track people with coronavirus," 2020. [Online]. Available: https://www.theguardian.com/australia-news/2020/apr/14/australian-government-plans-to-bring-in-mobile-phone-app-to-track-people-with-coronavirus

[22] B. Worthington, "Coronavirus tracing app covidsafe released by government to halt spread of covid-19 in australia," 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-26/coronavirus-tracing-app-covidsafe-australia-government-covid-19/12186130

[23] J. Hayne, "'no geolocation, no surveillance':government makes privacy assurances over coronavirus app," 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-18/prime-minister-rules-out-making-coronavirus-app-mandatory/12161126

[24] L. Besser and D. Welch, "Australians' data from covid-19 tracing app to be held by us cloud giant amazon," 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682

[25] jgould, "Using metadata to prosecute illegal sign usage is "overkill"," 2014. [Online]. Available: https://www.qt.com.au/news/petersen-slams-the-council-on-metadata/2423437/

[26] S. Hickey and U. Nedim, "Afp admits accessing metadata of australians 20,000 times in a year," 2019. [Online]. Available: https://www.sydneycriminallawyers.com.au/blog/afp-admits-accessing-metadata-of-australians-20000-times-in-a-year/

[27] P. Karp, "High court rules afp warrant for raid on news corp journalist's home was invalid," 2020. [Online]. Available: https://www.theguardian.com/australia-news/2020/apr/15/high-court-rules-afp-warrant-for-raid-on-news-corp-journalists-home-was-invalid

[28] A. Henderson, “Fears ‘fairly sophisticated actor’ hacked defence force database,” 2020. [Online]. Available: https://www.abc.net.au/news/2020-03-04/australian-defence-military-database-shut-down-amid-hack-fears/12021742

[29] S. Dalzell, “Getting australians to use government-sponsored coronavirus-tracing app a daunting exercise in persuasion,” 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-15/challenge-to-convince-australians-to-use-coronavirus-tracing-app/12151130

[30] I. Lane, “What draconian new coronavirus laws mean for our civil liberties,” 2020. [Online]. Available: https://thenewdaily.com.au/news/crime-news/2020/03/31/draconian-coronavirus-laws-australia/

[31] A. Probyn, “Coronavirus lockdowns could end in months if australians are willing to have their movements monitored,” 2020. [Online]. Available: https://www.abc.net.au/news/2020-04-14/coronavirus-app-government-wants-australians-to-download/12148210

[32] A. Barbaschow, “Australia looks to ‘go harder’ with use of covid-19 contact tracing app,” 2020. [Online]. Available: https://www.zdnet.com/article/australia-looks-to-go-harder-with-use-of-covid-19-contact-tracing-app/

[33] TraceTogether, “Team tracetogether.” 2020. [Online]. Available: https://tracetogether.zendesk.com/hc/en-sg

[34] ghuntley, “Covidsafe 1.0.11 apk,” 2020. [Online]. Available: https://github.com/ghuntley/COVIDSafe_1.0.11.apk

[35] D. J. Solove, “I’ve got nothing to hide and other misunderstandings of privacy,” *San Diego Law Review*, vol. 44, p. 745, 2007. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565

[36] G. DellAriccia, P. Mauro, A. Spilimbergo, and J. Zettelmeyer, “Economic policies for the covid-19 war,” 2020. [Online]. Available: https://blogs.imf.org/2020/04/01/economic-policies-for-the-covid-19-war/

[37] G. Goggin, A. Vromen, K. G. Weatherall, F. Martin, A. Webb, L. Sunman, and F. Bailo, “Digital rights in australia,” *Digital Rights in Australia (2017) ISBN-13*, pp. 978–0, 2017.

[38] M. Goerzen, E. A. Watkins, and G. Lim, “Entanglements and exploits: Sociotechnical security as an analytic framework,” in *9th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 19)*, 2019.

[39] BlueTrace, “Bluetrace manifesto.” 2020. [Online]. Available: http://tracetogether.zendesk.com/hc/en-sg/articles/360044883814

[40] J. Bay, J. Kek, A. Tan, C. S. Hau, L. Yongquan, and J. Tan, “Bluetrace: A privacy-preserving protocol for community-driven contact tracing across borders,” 2020. [Online]. Available: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

[41] H. Nissenbaum, “Privacy in context: Technology, policy, and the integrity of social life,” 2020. [Online]. Available: http://www.sup.org/books/title/?id=8862

[42] J. Gramenz, “Coronavirus australia: Covidsafe app hoax texts start circulating.”

[43] “Singapore personal data hack hits 1.5m,” 2018. [Online]. Available: https://www.bbc.com/news/world-asia-44900507

[44] “Coronavirus: Australian governments collecting phone location data.” 2020. [Online]. Available: https://thenewdaily.com.au/life/tech/2020/04/06/coronavirus-phone-location-tracking-data/

[45] G. R. Webb and F. R. Chevreau, “Planning to improvise: the importance of creativity and flexibility in crisis response,” *International Journal of Emergency Management*, vol. 3, no. 1, p. 66, 2006. [Online]. Available: https://doi.org/10.1504/ijem.2006.010282

[46] C. Jackson, “Tracetogether, singaporean covid-19 contact tracing and australian recommendations,” 2020. [Online]. Available: https://eng.unimelb.edu.au/ingenium/research-stories/world-class-research/real-world-impact/on-the-privacy-of-tracetogether,-the-singaporean-covid-19-contact-tracing-mobile-app,-and-recommendations-for-australia

[47] E. Strickland, “An official who coronavirus app will be a ‘waze for covid-19’,” 2020. [Online]. Available: https://spectrum.ieee.org/the-human-os/biomedical/devices/who-official-coronavirus-app-waze-covid19

[48] B. Gates, “How to respond to covid-19,” 2020. [Online]. Available: https://www.gatesnotes.com/Health/How-to-respond-to-COVID-19

[49] U. W. H. Organisation, “Worldhealthorganization/app,” 2020. [Online]. Available: https://github.com/WorldHealthOrganization/app

[50] eHealth Network, “Covid-19 apps,” 2020. [Online]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[51] A. Narayanan and V. Shmatikov, “De-anonymizing social networks,” in *2009 30th IEEE Symposium on Security and Privacy*, 2009, pp. 173–187.

[52] D. Pegg and P. Lewis, “Nhs coronavirus app: Memo discussed giving ministers power to ‘de-anonymise’ users,” 2020. [Online]. Available: https://www.theguardian.com/world/2020/apr/13/nhs-coronavirus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users

[53] F. Sainz, “Apple and google partner on covid-19 contact tracing technology,” 2020. [Online]. Available: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[54] F. Palamara, “Accc to sue google over location data - the market herald,” 2019. [Online]. Available: https://themarketherald.com.au/accc-to-sue-google-what-you-need-to-know-2019-10-29/

[55] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, “The dark (patterns) side of UX design,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI 18*. ACM Press, 2018. [Online]. Available: https://doi.org/10.1145/3173574.3174108

[56] “Telecommunications (interception and access) amendment (data retention) bill 2015,” 2020. [Online]. Available: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5375

[57] L. Lessig, *Code and Other Laws of Cyberspace*. USA: Basic Books, Inc., 1999.

[58] “Joint civil society statement: States use of digital surveillance technologies to fight pandemic must respect human rights,” 2020. [Online]. Available: https://newamericadotorg.s3.amazonaws.com/documents/Joint-statement-COVID-19-and-surveillance.pdf

[59] S. L. Star and K. Ruhleder, “Steps toward an ecology of infrastructure: Design and access for large information spaces,” *Information systems research*, vol. 7, no. 1, pp. 111–134, 1996.

[60] T. Altuwaiyan, M. Hadian, and X. Liang, “Epic: Efficient privacy-preserving contact tracing for infection detection,” in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[61] D. Winder, “United nations confirms ‘serious’ cyberattack with 42 core servers compromised,” 2020. [Online]. Available: https://www.forbes.com/sites/daveywinder/2020/01/30/united-nations-confirms-serious-cyberattack-with-42-core-servers-compromised/

[62] C. of Australia, “The assistance and access act 2018.” 2020. [Online]. Available: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[63] linus, “10 requirements for the evaluation of ‘contact tracing’ apps,” 2020. [Online]. Available: https://www.ccc.de/en/updates/2020/contact-tracing-requirements

[64] T. T. Coalition, “Tcn coalition a global coalition for privacy-first digital contact tracing protocols tofight covid-19.” 2020. [Online]. Available: https://tcn-coalition.org/

[65] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” *Journal of Cryptology*, vol. 1, no. 2, pp. 77–94, jun 1988. [Online]. Available: https://doi.org/10.1007/bf02351717

[66] “Private kit: Safe paths; privacy-by-design contact tracing,” 2020. [Online]. Available: http://safepaths.mit.edu/

[67] A. Greenberg, “Clever cryptography could protect privacy in covid-19 contact-tracing apps,” 2020. [Online]. Available: https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/

[68] H. Cho, D. Ippolito, and Y. W. Yu, “Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs,” Mar 2020. [Online]. Available: http://arxiv.org/abs/2003.11511v2

[69] B. Huang, “Simmel,” 2020. [Online]. Available: https://simmel.betrusted.io/

[70] F. Brunton and H. Nissenbaum, “Obfuscation,” 2020. [Online]. Available: https://mitpress.mit.edu/books/obfuscation

[71] S. B. Franklin, “New america foundation statement for the record,” 2020. [Online]. Available: https://newamericadotorg.s3.amazonaws.com/documents/New_Americas_Open_Technology_Institute_Statement_for_the_Record.pdf

[72] S. Star and K. Ruhleder, “Steps toward an ecology of infrastructure: Design and access for large information spaces,” *Information Systems Research*, vol. 7, pp. 111–134, 03 1996.

[73] F. Alvarez, M. Hollick, and P. Gardner-Stephen, “Maintaining both availability and integrity of communications: Challenges and guidelines for data security and privacy during disasters and crises,” in *2016 IEEE Global Humanitarian Technology Conference (GHTC)*. IEEE, 2016, pp. 62–70.