What Happens to COVID-19 Data After the Pandemic? Socio-Technical Lessons

***Abstract*—The COVID-19 global pandemic outbreak meant a complete reevaluation of societal interactions, business processes, and government policies. For decades, the scientific and technical communities had contemplated the possibility of an all-out airborne virus and had postulated how technology might be used in response, for example, in the reduction of transmission rates. In this paper, we examine the Australian COVID-19 technological response, focused initially on using a contact tracing app that would continually be broadcasting for known recorded cases, one nearby smartphone to another, and to the successive deployment of a QR-code-based solution requiring checking in and checking out of a place of congregation, like a closed or open campus setting. Despite the lackluster outcomes of the high-fidelity solutions, government continued, and in some instances, persisted in relying on QR codes for a considerable period. These solutions necessitated the collection of data pertaining to an individual for functioning, prompting a series of questions regarding the collection, storage, dissemination, and use of this data, both at the height of the pandemic and presently. On reflection, was the data effectively used or integrated into the proposed processes? Could the data be utilized in an unauthorized manner? And how might we circumvent its unauthorized use moving forward? Are there any potentially positive use cases that we could envisage? And, significantly, in the context of this piece, what are the broader socio-technical lessons or learnings that could be derived from such implementations that can be reinstituted into the design of future health-oriented systems? This paper provides an overview of Australia's contact tracing app, from here on referred to as COVIDSafe, and the subsequent use of QR Codes that were state based and governed by the Services arm of the Australian Government, to present design insights relevant to both the Australian context and beyond.**

***Index Terms*—COVID-19, data, data collection, use, access, privacy, security, retrospective use, scope creep, function creep, socio-technical, laws, regulations.**

I. Contact Tracing Apps: Australia's COVIDSafe

CONTACT tracing is not new. In 2017, the World Health Organization (WHO) identified three basic steps to any form of contact tracing: contact identification, contact listing, and follow-up [1]. Due to the COVID-19 pandemic, the topic of contact tracing became the subject of much debate as governments across the world sought to explore the role of technology in automating, semi-automating and or augmenting contact tracing processes. Some of these digitally transformed processes, not only attempted a 'trace' but also a 'track', meaning Bluetooth was used to determine when two smartphones came into proximity (about 1.5 meters apart), and automatic location identification was used to mark an end-user's position [2]. The aim of these apps was to perform health surveillance, which could help governments respond to the coronavirus crisis by proactively identifying and placing confirmed and suspected cases in quarantine [3], [4]. Data from these apps generally were stored for a predefined time, 14-21 days in the Australian context for COVIDSafe, to help monitor and ideally contain the spread of the disease [5]. With respect to uptake, a range of considerations inevitably influenced citizens' decisions to utilize the app. For example, public deliberations in Australia pointed to issues such as privacy, trust, voluntariness, proportionality, and fairness, among others as playing a key role in an individual's willingness to use contact tracing apps such as COVIDSafe [6]. But most contact tracing apps [7], [8] of this nature did not live up to expectations despite being touted as state-of-the-art technology [9], [10]. The apps, for many nations that simply relied on the Bluetooth sensor, demonstrated a case of how *not* to build socio-technical systems, mostly due to a lack of public consultation [11] and a lack of extensive testing of a prototype prior to deployment, in addition to many other pertinent considerations relevant to accounting, accountability and the calculative nature of digital technologies that remained unaddressed [12].

II. QR Codes: Checking in and Checking Out

As the pandemic continued, and lockdowns were relaxed in Australia, the next wave of technological intervention was introduced in the form of solutions utilizing QR codes, which were instituted on a state-by-state basis, whereby data was to be retained for up to 28 days (Fig. 1). These solutions were less about continuous tracking and more about the identification of individual patrons and small groups (e.g., dependents, family members, friends) that frequented a premises or venue. For example, in NSW, it was mandatory for people to check-in at the following businesses: retail stores and supermarkets; individual shops within shopping centers; gymnasiums; offices, including call centers; and manufacturers and warehouses. Institutions were not exempt, inclusive of universities and colleges and schools including teachers and visitors (such as parents and contractors) but excluding students [13]. Businesses such as hospitality and hairdressers that were already using the QR code had to also ensure the check-in of staff and visitors, such as maintenance workers and delivery drivers. Even hospitality businesses had to extend the use of the Service NSW COVIDSafe check-in to all customers including for takeaway orders. If any business was found in breach of compliance to these health order requirements, they would be subject to fines and even temporary closure [14].

By default, a venue is a fixed location with a civic address that can be converted to a geodetic address. So, while it

Digital Object Identifier 10.1109/TTS.2022.3226119

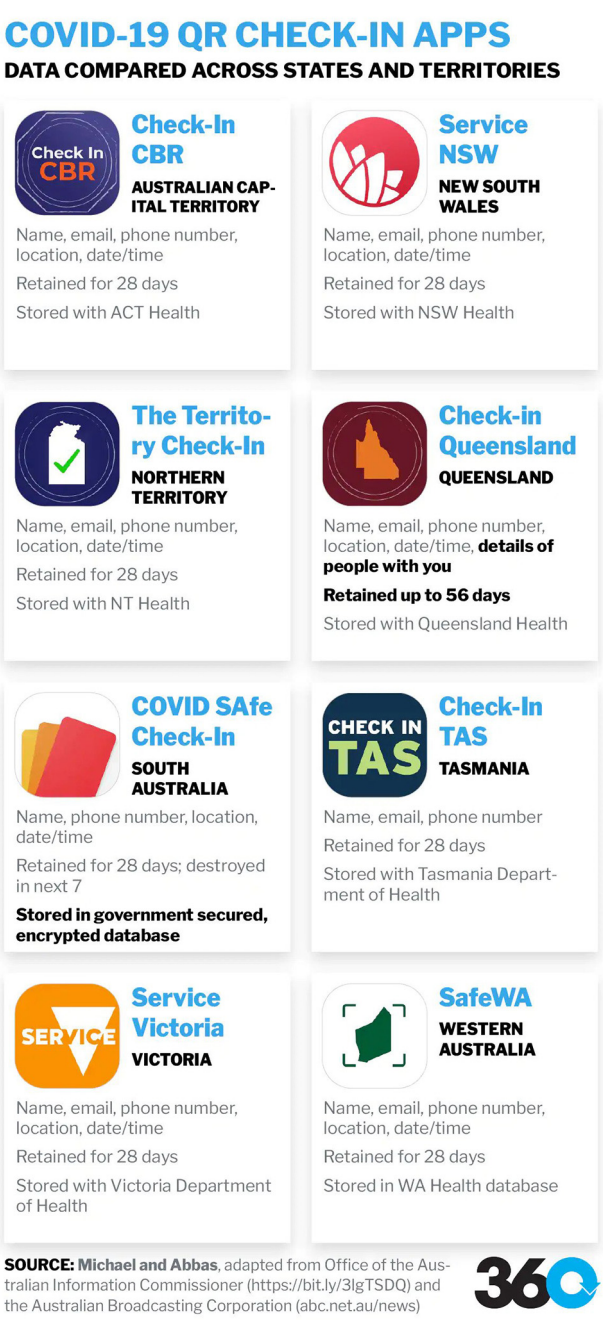

Fig. 1. COVID-19 QR code data compared across Australian states and territories. Courtesy of 360info™ [15].

seemed the government was merely interested in collecting identity information, the location of a venue was implicit. Many Australians who came out of lockdown, having felt isolated during the COVID experience, traded their personal information for the right to exercise their freedom to move in public and semi-public spaces. Australians, comparatively to previous contexts, shared disproportionately more data during the pandemic than they would have ordinarily been comfortable in sharing, simply to gain the right to enter a supermarket or frequent a café. As noted, state-level Quick Response (QR) code mandates [16] required people to check-in and out everywhere, even at the entrance of children's playgrounds, libraries, national parks, and other remote spaces (Figure 2).

Fig. 2. Top: QR Code Check-In and COVIDSafe Information at Ben Boyd National Park, NSW. Bottom: QR Code Check-In at Severs Beach. Courtesy of Katina Michael 14 December 2020.

These QR-code measures were intended to notify people who had come into proximity with a confirmed COVID-19 case, but it also came at a price: citizens were handing over an unprecedented amount of sensitive information to governments — their name, their location at a specific date and time and, often, details of accompanying dependents [17], and all of this digitally through a government mandated app. Groups gathering in small numbers of 3-4 would often register on a single handset, utilizing a single check-in submission, thus somewhat (unsuspectingly) sharing their physical social network as well.

Databanks like these for COVID-19 application should be stored securely and governed carefully, given the collection of personally identifiable information (PII) [18]. This has not been the case in general, and Australia was certainly not alone in the "deploy now, address issues later" approach. Laws surrounding the mandatory collection of data gathered by QR code-based check-ins have either come "after the fact" or have not been communicated well to the public [19].

III. Differentiating QR Code Types By Service Provider

While it was mandatory for businesses to record customer visits during COVID, they could opt to choose from a small number of implementation options. Initially there was great confusion among, for example, café owners regarding the state-based directives they would have to comply with, such as having an attendant at the front of the store [20], or ensuring that only people who had a vaccination certificate and who were willing to record at least their name and mobile

phone number could gain access to the café [21]. Additionally, businesses who were not digitally equipped felt particularly alienated by the process of which they as the merchant would have to bear the cost of any QR Code digital systems implementation. Some employers also created their own internal systems to ensure workers had checked-in and out from the company's physical premises.

Notwithstanding the possibility of government penalties on business owners, certain businesses opted for what they perceived to be suitable and or cheap third-party solutions, which resulted in a host of custom QR code based options and a multitude of service providers, before an 'official' Government solution was made available. For example, third-party suppliers, MyGuestList and ImpactData [22], stored tens of millions of check-ins on their databases by developing their own custom check-in apps using the state government's Application Programming Interface (API) [23]. These third-party solutions are not without their own risks. That is, there was nothing to prevent private companies from exploiting data collected for the purposes of COVID-19 to be used for their own benefit [24], or their clients' benefit. The law in Australia, for instance, does not prohibit these entities from analyzing the collected data to determine users' spending patterns [25], if the business's annual turnover is less than $3 million a year [26].

Australians who have broadly complied with this new level of monitoring may do so because of the public health imperative, but also because of assurances made by governments. Citizens were informed by government bodies [27] that their data would be safe, but there have been demonstrated breaches of trust. For example, after repeated claims [28] that QR code check-in apps would retain data for only 28 days, SA Health breached its own guidelines, storing QR code data indefinitely until an audit discovered the error alleged to be unintentional [29]. It is reported that on at least six occasions, [30] state police forces in Australia (e.g., Western Australian Police [31] without a search warrant and Queensland Police [32] with a search warrant) accessed check-in data for criminal investigations after assurances this would not be permitted. Victoria Police [33] also attempted to access the data and were prevented from doing so.

In a positive development, some states (e.g., NSW) [34] introduced laws preventing the retrospective or secondary use of COVID QR code data. The Service NSW (One-stop Access to Government Services) Amendment (COVID-19 Information Privacy) Bill 2021 came into effect in November 2021 [35], over a year after the COVID check-in mandate was introduced in October 2020, and five months after the extended mandate [13]. However, Australians who first raised alarm over whether their COVID-19 check-in data was being housed on servers in the United States — which was purportedly the case for the federal government's COVIDSafe app [36] — are still waiting for clarification, though the debate has somewhat shifted post lockdown. Yet, storing Australian data in the United States would subject Australians to the Cloud Act, American legislation that allows personal information to be accessed under subpoena. Legislative and regulatory considerations of this nature were not always explicitly conveyed. This challenge is not new, as Australia and other nation states have encountered similar ambiguity and lack of clarity regarding the regulatory landscape and legislative requirements; for instance in response to emergencies and other scenarios in the context of location-based services [51], [52].

With respect to the COVID-19 context, this lack of clarity and transparency was of concern given how much personal information had been stored: within four months of launching in Oct. 2020, for example, the Service NSW app lodged 30 million check-ins [37] noting the population of NSW at the time was 8.172 million. Indicative numbers for Service NSW report 50.6 million check-ins [23] in May 2021 alone. With a population of 6.62 million, Victoria, that experienced significantly longer lockdown measures beyond that of NSW, an estimated 18 million check-ins [23] were recorded in the fortnight of May 13 and May 31, 2021. This number grew over time in Victoria as more people returned to work, to 24.2 million check-ins in the first week of October 2021, and 25.2 million in the second week of October 2021. Furthermore, weekly check-ins rose to over 40 million in November and to over 45 million in December when lockdowns were ended [38]. According to the Department of Health in Victoria, the number of check-ins plummeted in mid-January to mid-February 2022, when only about 20 million check-ins were registered weekly until the app was abandoned as people became complacent about checking-in and perhaps suspicious about why the data was still being collected when COVID-19 cases had diminished.

Still, all of this continued compliance by citizens, amounted to billions of data points of Australians' whereabouts and other potentially sensitive details being collected, if we count just Victoria and NSW, while the QRCode was actively in operation. A concern in this regard is that not only did citizens provide data that linked their identity to their movements on the app [39], but they at times also offered the identities of dependents when checking in on behalf of family members or friends. If there was a major hack of any of the state's major cloud service providers, this data would be compromised. It would provide the capability to potentially create a web of cyber-physical-social connections unforeseen in Australia's history, beyond the most recent Optus [40] and Medibank Private [41] data breaches.

IV. Lessons Learned Moving Forward

The perceived shortcomings and lack of transparency concerning data, in addition to the absence of clarity in communication / awareness campaigns regarding the use and implementation of both COVIDSafe and the QR code-based solutions in Australia, provide valuable insights regarding the future design of socio-technical systems that are in the public interest [42]. These lessons apply beyond the Australian context, to a global setting and can potentially inform future socio-technical interventions in times of crisis but also more broadly, in order to promote the responsible design and development of technology toward desirable and positive use cases, that preserve and are in alignment with fundamental values such as privacy.

For instance, lessons regarding transparency with respect to data can be observed in the example of the QR code solution, whereby data storage related concerns and perceived lack of

transparency partly arose from public health directives delivered hastily. This resulted in businesses scrambling to figure out how they would address new government rules, with very little notice or guidance, before more prescriptive directions were delivered [43].

This is a major lesson for the government, organizations, and the Australian public to be better prepared for technology rollouts during periods of emergency declaration or disaster [44], [45], [53], [54]. Australia has experience using apps and visualization dashboards in its bushfire history, for example, the Rural Fire Service's app, FiresNearMe [46]. This preparedness requires not only learning from previous successful and unsuccessful instances of deployment, but also engaging in consultative and participatory processes during the crises, as well as prior to technology design and development efforts, by establishing mechanisms to capture both professional expertise relevant to a given crisis but also the lived experience and requirements of citizens [42], [55], [56].

This proposed approach ensures that potential socio-technical challenges can be identified and addressed prior to implementation to avoid challenges that were encountered during the COVID-19 pandemic. For instance, the COVIDSafe app implementation demonstrated issues of accessibility [23] and the QR code system rollout overlooked inclusivity, for example it did not account for those living with vision impairment [47]. Such issues likely would have been identified through consultative and participatory approaches to solution design.

This paper, and the lessons learned from the Australian case study presented within, also suggests that suitable governance frameworks are necessary to harness the power of technology in the public interest [42]. This point requires further reflection, attention and the commitment of multiple stakeholders. It is everyone's responsibility [48]. While new technologies are not silver bullet solutions, we are able to draw on our experience of technological responses in the context of the pandemic and other associated cases of implementation, to enhance our approach to socio-technical systems design and development in a given (national or community) context [57].

In the case of Australia, it was demonstrated that stakeholders must be more considered in their actions, as they chart a course toward a post-pandemic life. Actions relevant to data collected during the pandemic, and applicable beyond the Australian setting, require governments and other stakeholders to ponder and answer persisting questions, the major question being: Moving forward, what will happen to the gathered data [58]?

V. Conclusion

This question and others must be contemplated and resolved to avoid technological solutions, systems, and other processes and measures, introduced during the pandemic becoming default mechanisms after the public health crisis ends. Furthermore, we need to avoid normalizing certain actions that will eventually become "habits" for citizens and other stakeholders alike. For instance, when states terminated check-in mandates after vaccination rates reached 95 percent in New South Wales, Australia [49], the challenge of breaking this ingrained habit of checking in on "auto-pilot" began. It demonstrated that once a process had been digitally transformed and normalized it was difficult to return to the status quo. For many, handing over sensitive data already feels like an obligatory action, like wearing a mask in a healthcare facility. However, citizens need to be made aware of their rights and we need to learn from this experience, deliberately and concertedly drawing on the socio-technical lessons and insights from this experience to inform, enhance and adapt existing technology design and development processes.

References

[1] "Infection prevention and control: Contact tracing." World Health Organization. May 2017. [Online]. Available: https://www.who.int/news-room/questions-and-answers/item/contact-tracing

[2] J. Boyd. "Australia's contact-tracing COVIDSafe app off to a fast start." IEEE Spectrum. May 2020. [Online]. Available: https://spectrum.ieee.org/tech-talk/computing/software/australias-contact-tracing-covidsafe-app

[3] H. Thapliyal, K. Michael, S. P. Mohanty, M. B. Srinivas, and M. K. Ganapathiraju, "Consumer technology-based solutions for COVID-19," *IEEE Consum. Electron. Mag.*, vol. 10, no. 2, pp. 64–65, Mar. 2021, doi: 10.1109/MCE.2020.3040513.

[4] K. Michael, B. Stroh, O. Berry, A. Muhlhauber, and T. Nicholls, "The AVIAN flu tracker—A location service proof of concept," in *Proc. Recent Adv. Security Technol. RNSA Security Technol. Conf.*, Canberra, ACT, Australia, Sep. 2006, p. 387.

[5] R. Abbas and K. Michael. "The coronavirus contact tracing app won't log your location, but it will reveal who you hang out with." The Conversation. Apr. 2020. [Online]. Available: https://theconversation.com/the-coronavirus-contact-tracing-app-wont-log-your-location-but-it-will-reveal-who-you-hang-out-with-136387

[6] C. Degeling, J. Hall, J. Johnson, R. Abbas, S. Bag, and G. L. Gilbert, "Should digital contact tracing technologies be used to control COVID-19? perspectives from an Australian public deliberation," *Health Care Anal.*, vol. 30, pp. 97–114, Jun. 2022. [Online]. Available: https://doi.org/10.1007/s10728-021-00441-1

[7] R. Abbas and K. Michael, "COVID-19 contact trace app deployments: Learnings from Australia and Singapore," *IEEE Consum. Electron. Mag.*, vol. 9, no. 5, pp. 65–70, Sep. 2020, doi: 10.1109/MCE.2020.3002490.

[8] K. Michael and R. Abbas, "Behind COVID-19 contact trace apps: The Google–Apple partnership," *IEEE Consum. Electron. Mag.*, vol. 9, no. 5, pp. 71–76, Sep. 2020, doi: 10.1109/MCE.2020.3002492.

[9] K. Kolasa, F. Mazzi, E. Leszczuk-Czubkowska, Z. Zrubka, and M. Péntek, "State of the art in adoption of contact tracing apps and recommendations regarding privacy protection and public health: Systematic review," *JMIR Mhealth Uhealth*, vol. 9, no. 6, Jun. 2021, Art. no. e23250, doi: 10.2196/23250.

[10] A. Blasimme, A. Ferretti, and E. Vayena, "Digital contact tracing against COVID-19 in Europe: Current features and ongoing developments," *Front. Digit. Health*, vol. 3, Jun. 2021, Art. no. 660823, doi: 10.3389/fdgth.2021.660823.

[11] K. Michael, R. Abbas, R. Nicholls, J. Carvalko, and S. W. Fosso, "The impacts of mobile technology and regulation in a pandemic," in *Proc. AAAS Annu. Meeting*, Feb. 2021.

[12] E. J. Twyford and R. Abbas, "Broadening the boundaries of accounting: A call for interdisciplinarity in the calculative era," *Meditari Accountancy Res.*, to be published. [Online]. Available: https://doi.org/10.1108/MEDAR-06-2021-1338

[13] "COVID check-in mandate expanded." MyServiceNSW. Jun. 2021. [Online]. Available: https://www.nsw.gov.au/media-releases/covid-check-mandate-expanded

[14] F. Hunter. "Nine Sydney businesses fined for COVID-19 breaches during targeted police operation." The Sydney Morning Herald. Feb. 2021. [Online]. Available: https://www.smh.com.au/national/nsw/nine-sydney-businesses-fined-for-covid-19-breaches-during-targeted-police-operation-20210207-p570cj.html

[15] K. Michael and R. Abbas. "What will happen to all our COVID-19 data after the pandemic?" SBS News. 2022. [Online]. Available: https://www.sbs.com.au/news/article/what-will-happen-to-all-our-covid-19-data-after-the-pandemic/1379opfpy

[16] "Mandatory electronic check-in." NSW Government. Oct. 2021. [Online]. Available: https://www.nsw.gov.au/covid-19/business/check-in/mandatory-qr-code

[17] Service NSW. "COVID safe check-in (businesses)—FAQs." NSW Government. Jul. 2021. [Online]. Available: https://www.service.nsw.gov.au/covid-safe-check-businesses-faqs

[18] G. Greenleaf and K. Kemp. "Police access to COVID check-in data is an affront to our privacy. We need stronger and more consistent rules in place." The Conversation. Sep. 2021. [Online]. Available: https://theconversation.com/police-access-to-covid-check-in-data-is-an-affront-to-our-privacy-we-need-stronger-and-more-consistent-rules-in-place-167360

[19] RMIT ABC Fact Check. "No, requiring people to check in with a QR code does not breach Australian law." ABC News Covid Blog. Nov. 2021. [Online]. Available: https://www.abc.net.au/news/2021-11-05/coronacheck-qr-codes-do-not-breach-australian-law/100593754

[20] J. Purtill. "The proliferation of QR code check-ins is a 'dog's breakfast'. Is there a better way?" ABC News Covid Blog. Nov. 2020. [Online]. Available: https://www.abc.net.au/news/science/2020-11-20/covid-19-coronavirus-why-so-many-qr-code-check-in-systems/12895678

[21] J. Cartwright. "All NSW businesses must use Service NSW QR codes by Jan 1st or face $5k fine." techAU. 2007. [Online]. Available: https://techau.com.au/nsw-businesses-must-use-service-nsw-qr-codes-by-jan-1st-or-face-5k-fine

[22] K. Nguyen. "The QR code has turned COVID-19 check-ins into a golden opportunity for marketing and data companies." ABC News Covid Blog. Oct. 2020. [Online]. Available: https://www.abc.net.au/news/2020-10-31/covid-19-check-in-data-using-qr-codes-raises-privacy-concerns/12823432

[23] J. Taylor. "Victoria makes Covid check-in mandatory at shops after transmissions from 'fleeting' visits." The Guardian. Jun. 2021. [Online]. Available: https://www.theguardian.com/australia-news/2021/jun/02/victoria-makes-covid-check-in-mandatory-at-shops-after-transmissions-from-fleeting-visits

[24] S. Bradshaw and E. Dickens. "Using a QR code for COVID-safe check-in to your business premises? Five tips for staying privacy safe, too." Clayton Utz. Oct. 2020. [Online]. Available: https://www.claytonutz.com/knowledge/2020/october/using-a-qr-code-for-covid-safe-check-in-to-your-business-premises-five-tips-for-staying-privacy-safe-too

[25] S. Millward. "QR codes: Where did all your data go?" Smrtr. 2021. [Online]. Available: https://www.smrtr.com.au/news-views/qr-codes-where-did-all-your-data-go/

[26] OAIC. "The privacy act 1988." Australian Government. 1988. [Online]. Available: https://www.oaic.gov.au/privacy/the-privacy-act

[27] Service. "Our privacy and security policy." Victoria State Government. 2021. [Online]. Available: https://service.vic.gov.au/privacy-and-security

[28] Covid Blog. "QR codes are being rolled out in venues across South Australia—Here's what you need to know." ABC News. Dec. 2020. [Online]. Available: https://www.abc.net.au/news/2020-12-01/what-you-need-to-know-about-covid-qr-codes-in-south-australia/12937756

[29] I. Dayman. "SA Health holding QR code check-in data indefinitely, report finds, as risk of breach revealed." ABC News. Oct. 2021. [Online]. Available: https://www.abc.net.au/news/2021-10-12/sa-qr-check-in-data-audit/100533790

[30] A. Galloway. "'Breach of trust': Police using QR check-in data to solve crimes." Sydney Morning Herald. Sep. 2021. [Online]. Available: https://www.smh.com.au/politics/federal/breach-of-trust-police-using-qr-check-in-data-to-solve-crimes-20210903-p58om8.html?btis

[31] K. Png. "Police would not agree to stop accessing COVID SafeWA data, Premier Mark McGowan says." ABC News Covid Blog. Jun. 2021. [Online]. Available: https://www.abc.net.au/news/2021-06-16/police-refused-to-stop-accessing-safewa-app-data-premier-says/100218764

[32] "Calls for police to be barred from snooping on QR code check-in data." news.com.au. Sep. 2021. [Online]. Available: https://www.news.com.au/technology/online/security/calls-for-police-to-be-barred-from-snooping-on-qr-code-checkin-data/news-story/02eaa0ef19912b05724ba43dea1c66f2

[33] M. Fowler. "Police sought access to QR check-in data intended for contact tracing." The Age. Jun. 2021. [Online]. Available: https://www.theage.com.au/politics/victoria/police-sought-access-to-qr-check-in-data-intended-for-contact-tracing-20210621-p582x4.html

[34] A. Singh. "Police banned from accessing QR code data." Lexology. Nov. 2021. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=0cfda914-29ef-4e8d-99f7-ad7349147481

[35] "Service NSW (one-stop access to government services) amendment (COVID-19 information privacy) bill 2021." Parliament NSW. Nov. 2021. [Online]. Available: https://www.parliament.nsw.gov.au/bills/Pages/bill-details.aspx?pk=3914

[36] D. Welch and L. Besser. "Experts warn there are still legal ways the U.S. could obtain COVIDSafe data." ABC News Covid Blog. Apr. 2021. [Online]. Available: https://www.abc.net.au/news/2020-04-28/covidsafe-tracing-app-data-may-not-be-protected-from-usa/12189372

[37] A. Barbaschow. "Over 30 million 'Covid safe' check-ins through the service NSW app." ZDNet. Jan. 2021. [Online]. Available: https://www.zdnet.com/article/over-30-million-covid-safe-check-ins-through-service-nsws-app/

[38] T. Cowie and R. Eddie. "Victorians abandon QR code check-ins as COVID cases drop." The Age. Feb. 2022. [Online]. Available: https://www.theage.com.au/national/victoria/victorians-abandon-qr-code-check-ins-as-covid-cases-drop-20220211-p59vnr.html

[39] W. Aly. "Police accessing QR data violates our emergency pact." The Sydney Morning Herald. Sep. 2021. [Online]. Available: https://www.smh.com.au/national/police-accessing-qr-data-violates-our-emergency-pact-20210909-p58q2f.html

[40] D. Kolevski, K. Michael, R. Abbas, and M. Freeman, "Cloud computing data breaches in news media: Disclosure of personal and sensitive data," in *Proc. IEEE Int. Symp. Technol. Soc.*, Hong Kong, Nov. 2022, pp. 1–11.

[41] C. Kruger. "AFP steps in as Medibank hack data migrates from dark Web." Sydney Morning Herald. Nov. 2022. [Online]. Available: https://www.smh.com.au/business/companies/medibank-faces-new-headaches-as-it-finds-staff-data-has-also-been-hacked-20221115-p5byap.html

[42] R. Abbas, J. Pitt, and K. Michael, "Socio-technical design for public interest technology," *IEEE Trans. Technol. Soc.*, vol. 2, no. 2, pp. 55–61, Jun. 2021, doi: 10.1109/TTS.2021.3086260.

[43] "Setting up electronic check-in and QR codes." NSW.gov.au. Jul. 2021. [Online]. Available: https://www.nsw.gov.au/covid-19/business/check-in/setting-up-electronic-check-and-qr-codes

[44] A. Aloudat, K. Michael, R. Abbas, and M. Al-Debei, "The value of government mandated location-based services in emergencies in Australia," *J. Inf. Technol. Res.*, vol. 4, no. 4, pp. 41–68, 2011. [Online]. Available: https://doi.org/10.4018/jitr.2011100103

[45] A. Aloudat and K. Michael, "Toward the regulation of ubiquitous mobile government: A case study on location-based emergency services in Australia," *Electron. Commerce Res.*, vol. 11, no. 1, pp. 31–74, 2011. [Online]. Available: https://doi.org/10.1007/s10660-010-9070-0

[46] "Fires Near Me NSW: Rural Fire Service app could save your life." Daily Telegraph. Nov. 2019. [Online]. Available: https://www.dailytelegraph.com.au/news/nsw/nsw-rural-fire-service-app-fires-near-me-will-keep-you-up-to-date-and-help-you-stay-safe/news-story/64219c78b685972bd6c9df0c8a96e488

[47] A. O'Flaherty. "QR codes should be 'more inclusive' for people with vision impairment." ABC News Covid Blog. Aug. 2021. [Online]. Available: https://www.abc.net.au/news/2021-08-16/calls-or-mandatory-covid-19-check-in-qr-codes-to-be-inclusive/100375590

[48] K. Michael, R. Abbas, and J. Pitt. "Maintaining Control Over AI." Issues in Science and Technology. 2021. [Online]. Available: https://issues.org/debating-human-control-over-artificial-intelligence-forum-shneiderman

[49] H. Parkes-Hupton. "NSW government updates roadmap for easing of COVID-19 restrictions after state reaches 95pc double dose vaccination target." ABC News. Nov. 2021. [Online]. Available: https://www.abc.net.au/news/2021-11-25/nsw-updates-roadmap-95-percent-double-dose-vaccination/100649860

[50] S. J. Fusco, K. Jean, M. G. Michael, and R. Abbas, "Exploring the social implications of location based social networking: An inquiry into the perceived positive and negative impacts of using LBSN between friends," in *Proc. 9th Int. Conf. Mobile Bus. 9th Global Mobility Roundtable*, Athens, Greece, 2010, pp. 230–237, doi: 10.1109/ICMB-GMR.2010.35.

[51] R. Abbas, K. Michael, M. G. Michael, and R. Nicholls, "Sketching and validating the location-based services (LBS) regulatory framework in Australia," *Comput. Law Security Rev.*, vol. 29, no. 5, pp. 576–589, 2013. [Online]. Available: https://doi.org/10.1016/j.clsr.2013.07.014

[52] R. Abbas, K. Michael, M. Michael, R. Nicholls, "Key government agency perspectives on location based services regulation," *Comput. Law Security Rev.*, vol. 31, no. 6, pp. 736–748, 2015. [Online]. Available: https://doi.org/10.1016/j.clsr.2015.08.004

[53] A. Aloudat and K. Michael, "The application of location based services in national emergency warning systems: SMS, cell broadcast services and beyond," in *Proc. Nat. Security Sci. Innov. Conf.*, Canberra, ACT, Australia, 2011, pp. 21–49.

[54] R. Abbas, K. Michael, and M. G. Michael, "The regulatory considerations and ethical dilemmas of location-based services (LBS) : A literature review," *Inf. Technol. People*, vol. 27 no. 1, pp. 2–20, 2014. [Online]. Available: https://doi.org/10.1108/ITP-12-2012-0156

[55] R. Abbas, S. Hamdoun, J. Abu-Ghazaleh, N. Chhetri, N. Chhetri, and K. Michael, "Co-designing the future with public interest technology," *IEEE Technol. Soc. Mag.*, vol. 40, no. 3, pp. 10–15, Sep. 2021, doi: 10.1109/MTS.2021.3101825.

[56] J. Caspermeyer. "Design and deployment of COVID-19 technology responses and finding ways to make things." EurekaAlert. Feb. 2021. [Online]. Available: https://www.eurekalert.org/pub_releases/2021-02/asu-dad020521.php

[57] K. Michael and M. G. Michael, Eds., *Australia and the New Technologies: Evidence Based Policy in Public Administration*. Canberra, ACT, Australia: Univ. Wollongong Press, 2008.

[58] R. Abbas, K. Michael, and M. G. Michael, "Using a social-ethical framework to evaluate location-based services in an Internet of Things world," *Int. Rev. Inf. Ethics*, vol. 22, pp. 42–73, Dec. 2014. [Online]. Available: https://doi.org/10.29173/irie118

KATINA MICHAEL, *Editor-in-Chief*
School for the Future of Innovation in Society
School of Computing and Augmented Intelligence
Arizona State University
Tempe, AZ 85281 USA
katina.michael@asu.edu

ROBA ABBAS, *Associate Editor*
School of Business
University of Wollongong
Wollongong, NSW 2522, Australia
roba@uow.edu.au

Katina Michael (Senior Member, IEEE) is a Professor with Arizona State University and a Senior Global Futures Scientist with the Global Futures Laboratory and has a joint appointment with the School for the Future of Innovation in Society and School of Computing and Augmented Intelligence. Prior to academia, she was employed by Nortel Networks, Anderson Consulting, and OTIS Elevator Company. She has been funded by the National Science Foundation, the Canadian Social Sciences and Humanities Research Council, and the Australian Research Council. She is the Director of the Society Policy Engineering Collective and the Founding Editor-in-Chief of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY. She is also the Founding Chair of the inaugural Masters of Science in Public Interest Technology.

Roba Abbas (Member, IEEE) is a Senior Lecturer of Operations and Systems and an Academic Program Director with the Faculty of Business and Law, University of Wollongong, Australia, and more recently a Visiting Professor with the School for the Future of Innovation in Society, Arizona State University, USA. Her research is focused on methodological approaches to complex socio-technical systems design, emphasizing transdisciplinarity, co-design and the intersection of society, technology, ethics, and regulation. She is also a Co-Editor of the IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, a Former Associate Editor of the *IEEE Technology and Society Magazine*, and the Technical Committee Chair of the Socio-Technical Systems Committee of the IEEE.