Legal preparedness in implementing digital contact tracing apps in managing public health threats: the Singapore experience

International Journal of Law in Context (2026), **22**, 60–74
doi:10.1017/S1744552325100372

SPECIAL ISSUE ARTICLE

Legal preparedness in implementing digital contact tracing apps in managing public health threats: the Singapore experience

Hui Yun Chan

University of Reading Malaysia, Iskandar Puteri, Malaysia
Email: huiyun.chan@reading.edu.my

(Received 27 November 2025; revised 27 November 2025; accepted 1 December 2025; first published online 14 January 2026)

Abstract

The introduction and use of digital contact tracing apps as part of pandemic management have notably raised many legal and ethical challenges, ranging from determinations of public interest in using gathered data to privacy protections for app users and broader considerations of national socio-economic priorities. As the use of these digital contact tracing apps is supported by laws, legal preparedness is essential in determining appropriate legal authority that considers necessary trade-offs such as temporary privacy infringements, proportional data gathering and collective public health benefits. This paper examines the extent of legal preparedness in addressing competing interests between public health and individuals in the use of digital contact tracing apps. It does so through two main lenses: (1) an analysis of Singapore's legal framework pertaining to data protection, privacy and contact tracing apps and (2) an analysis of the domestic social and political influences that explain why Singapore's approach to digital contact tracing was viable, and assess its potential or limits for broader applicability.

Keywords: digital contact tracing apps; legal preparedness; public interest; pandemic; privacy

1 Background: pandemic preparedness, digitalisation of contact tracing and the importance of legal preparedness

Pandemic preparedness has historical origins within civil defence and emergency management with a focus upon risk assessment, scenario-based planning, early warning systems and stockpiling of essentials (Amariles 2021, p. 7). Preparedness is an active, continuous process that envisions the management of threats through possibilities occurring, identifying existing vulnerabilities and creating responsibilities in mitigating those risks (Amariles 2021, pp. 15, 20). An example of vulnerability is consideration of the country's critical infrastructure interests such as the continued functioning of socio-economic life (Amariles 2021, pp. 30, 34). The level of preparedness is closely related to broader systems in the domestic preparedness chain, such as the supply and demand for physical items, regulatory systems that obstruct or facilitate preparedness, sociopolitical sentiments toward these preparatory initiatives and the environment.

Pandemic preparedness involves a range of mechanisms requiring coordinated efforts among a wide network of agencies and actors (local, international and the population). Physical preparedness often entails stockpiling of personal protective equipment, medicine, ventilators and hospital beds, and includes establishing border control and restricting movements of people. This aspect is often prioritised and could sometimes cross into over-preparedness. Other important

aspects of pandemic preparedness, such as legal preparedness, are often underdeveloped (IDLO 2023). Consequently, considerations of individuals' rights and interests such as potential risks of harm from surveillance through contact tracing apps and the broader impact of pandemic under-preparedness on the population become deprioritised. Examples of deficiencies in pandemic preparedness range from public health infrastructure and systems, low uptake and adoption of recommendations and gaps in international collaborations to pre-existing inequalities and challenges in regulatory approvals for medicine and marketing of vaccines (Driece *et al.* 2023). The lack of social and political readiness to prepare for pandemics is another contributing factor to under-preparedness (Ho 2022). Meanwhile, emergency laws governing contact tracing apps that contradict existing laws, or the lack of governmental-industry coordination in data protection requirements are examples of legal under-preparedness (Lund-Tønnesen and Christensen 2023, p. 136).

The International Health Regulations (IHR) serves as guidance for member states in pandemic preparedness, which include assessing national public health structures and surveillance capacities among others (WHO 2024). One of the key foci in implementing IHR principles is updating national legislation to operationalise IHR in domestic legal frameworks for implementing national measures (WHO 2024). This measure improves coordination between various parties in implementing IHR obligations and strengthens the exercise of rights in the IHR by the authorities (WHO 2024). A study by the International Federation of Red Cross (IFRC) has stressed the significance of trust, equity and local action as essential ingredients in public health preparedness, in addition to robust laws and policies as part of enhancing legal preparedness for future pandemic preparedness (IFRC 2023). The study calls for strengthening of legal preparedness through reviewing and updating the respective legal frameworks periodically and post-public health crises toward enabling an effective environment to address public health emergencies (IFRC 2023). Legal scholars in public health have echoed support for countries to build legal preparedness capacity as part of public health preparedness for future pandemics through the Global Health Security Agenda's Legal Preparedness Action Package (Ayala *et al.* 2022). It aims to develop and circulate legal resources in support of legal preparedness for countries around the world, including preparing for the development and implementation of emergency laws (Ayala *et al.* 2022). This is achieved through stakeholder engagement advocacy and outreach activities regarding the importance of legal preparedness, guidance tools for countries to improve legal preparedness that emphasise the value of local, national and international legal preparedness, and building capacity through establishing networks of experts and integrating legal standards toward legal preparedness (Ayala *et al.* 2022). The emphasis on legal preparedness as one of the core capacities under the IHR is evident in pandemic treaty negotiations, underscoring the significance of strengthening legal preparedness at all levels (Negri *et al.* 2024).

Digitalisation has transformed the way people work, live, connect and play (Cetron and Davies 1997; Condie and Dayton 2020). The Covid-19 pandemic has amplified the use of digital health and mobile applications, including wearables (Negreino 2021). The growth in digital surveillance and pandemic preparedness highlights an increasingly important tool in pandemic response strategies. These devices have enabled the dissemination of public health messaging, contact tracing or data sharing between national agencies and pharmaceutical companies for vaccine development. Apps are designed to function and interoperate with various hardware, thus covering broader aspects of people's lives that use digital infrastructure (Goggin and Zhuang 2023). The use of these applications thus raised concerns regarding surveillance, privacy, security flaws, equitable access to the benefits of these apps and legal preparedness in enabling data sharing for pandemic management. When data from population surveillance is misused, breaches of intrinsic personal interests could occur, consequently harming data subjects. Another key issue is the availability of appropriate laws to prevent data misuse and the power to make organisations accountable for data misuse (Summers *et al.* 2022). These

concerns are interlinked with broader sociopolitical and economic considerations in balancing competing public health benefits from contact tracing and governmental responsibilities in their implementation. Further, doubts exist regarding the efficacy and safety of these apps, due to a lack of a robust evidence base for their scientific validity and accuracy because of their speedy implementation and lack of testing and vetting (Hogan *et al.* 2021). More generally, regulatory frameworks governing digital health applications often trail innovations, and the regular legal landscape of light regulation dominant in non-emergency settings continues into an emergency. A responsible contact tracing data gathering model could be realised via legal frameworks that protect individual privacy, minimise data misuse and establish the scope and authority of governmental agencies in accessing and using collected information. Pandemic surveillance using digital health tools is usually compulsory during public health crises and often interferes with the usual functioning of individuals' lives. Other broader implications include people's willingness to share personal data, public trust in the receiving body, concerns regarding data misuse (Summers *et al.* 2022) and inequities in data sharing benefits (Pratt and Bull 2021). This paper explores the following question: what is the extent of legal preparedness in implementing digital contact tracing apps in the population? A recent definition of legal preparedness is 'the capability to map, develop, refine, and use legal instruments that enable the implementation of capacities across sectors to prevent, prepare for, respond to, and recover from health emergencies' (GHSA LP AP 2023; Negri *et al.* 2024). Legal preparedness, in the context of digital contact tracing apps can be understood as developing or refining legal frameworks governing contact tracing apps to realise the aims of contact tracing in containing the spread of infections in the community through establishing an appropriate scope of authorities, clarifying the method of deploying the apps, the actors involved in its development and implementation, as well as the stages and the context in which the use of these apps are mandated.

An examination of legal readiness is significant for two reasons. First, legal preparedness seems to be secondary to achieving the intended effects of deploying contact tracing apps for infection surveillance. However, there are broader social implications arising from emergency public health laws, the implementation of technological tools (e.g. risks to populations), societal readiness in accessing or adapting to these applications and any commercial interests in implementing these tools. Through an exploration of legal preparedness, the paper identifies important resulting tensions, concerns and trade-offs in using digital contact tracing apps during pandemics. Second, while governments are generally prepared in stockpiling masks and medicine, legal preparedness in surveillance frameworks using digital contact tracing apps remains underexplored. There are important long-term implications arising from this regulatory lacuna, such as considering how different values were weighed in Singapore and the lessons that can be learned, or identifying how population attitudes toward notions of privacy and the tensions with collective public health benefits have evolved over time. These are important factors influencing the success of legal preparedness in preparation for future pandemics. A socio-legal approach provides a context to understand the interaction between laws and society, such as identifying competing interests that arise – that is, balancing the benefits of contact tracing tools and safeguarding personal rights. Research has previously shown the significance of considering the impact of digital health applications using principles of necessity and proportionality and the role they ought to play in striking a balance between surveillance, public health protection and personal privacy (Sekalala *et al.* 2020). Contact tracing apps have highlighted neglected scrutiny of legal preparedness for fast-developing digital health applications.

While significant attention has been given to the potential risks of harm to individuals from data-intensive apps (Schroeder *et al.* 2022; Skirpan *et al.* 2018; Wykes and Schueller 2019), there has been less focus on the exigencies of pandemics where inevitable trade-offs are made to achieve public health goals. While Southeast Asian (SEA) countries have swiftly introduced digital contact

tracing apps, little is reported about their regulatory preparedness.[1] Singapore illustrates a unique SEA sociocultural demography within a high-income economic setting (compared to its SEA neighbours) and pre-existing social acceptance of political trade-offs in return for education and social goods promoted by a strong central government administration (Austin 2009; Stiftung 2024). Its increasingly ageing population and a heightened digital health surveillance nation, supported by regulatory mandates across the city-state during the pandemic, illustrate how the confluence of factors influences the extent of regulatory preparedness in implementing contact tracing apps for health surveillance.

This paper aims to explore the extent of legal preparedness in implementing digital contact tracing in the Singaporean population. It seeks to understand the Singapore approach toward legal preparedness and its viability, situated within the distinct social norms and political contexts of the nation. In the case of Singapore, the regulatory analysis showed that while some privacy concerns emerged, governmental approaches in normalising surveillance as part of protecting and prioritising national economic interests and maintaining the functioning of health care systems during pandemic times have influenced its public health approach in implementing nationwide digital contact tracing. The amendments to the Covid-19 (Temporary Measures) Act 2020 of Singapore that specifically restricted the use of contact tracing data for criminal investigation to serious offences reflected an attempt to balance collective health interests and individual concerns for privacy. Additionally, the legislative spirit for data protection is twofold, providing minimum standards for data protection and facilitating cross-border data flows in the economic interests of the nation. Moreover, the general attitude toward privacy can be gathered through the domestic court's rejection of privacy as understood in the predominant Eurocentric approaches that emphasise individual privacy and data protection. Interpreting privacy from the lens of human rights is inappropriate for the context of Singapore. Legal preparedness can be improved and optimised through aligning with population concerns for privacy and balancing national priorities in economic interests as a long-term strategy to address evolving privacy concerns.

The paper proceeds as follows. Section 1 provides an overview of broader pandemic preparedness efforts, the rise in digitalisation of contact tracing and the importance of legal preparedness. Section 2 describes the growth of digitalisation in Singapore, supported by a national move toward 'smart nation' that aims to harness benefits from digitalisation to provide a context for the discussion. This occurs within a distinct social, cultural and political context with emerging privacy awareness. It will reveal social attitudes toward privacy and the normalisation of privacy at the government level, thus shaping norms about privacy. Nonetheless, this approach does not exclude concerns regarding privacy from the population, raising questions about the use of public health data collected through digital contact tracing apps. The latter underscores the importance of legal preparedness in establishing appropriate boundaries in balancing competing interests between collective public health benefits and individual privacy concerns. Laws governing the use of digital contact tracing apps were adjusted to accommodate these public concerns, highlighting the opportunity to evaluate legal preparedness in addressing the challenges arising from implementing digital contact tracing. This is addressed in Section 3. Section 4 signposts some considerations for future pandemics, highlighting the potential and limitations for broader applications.

[1]There is a lack of direct references regarding studies on regulatory preparedness for contact tracing, hence the opportunity to explore the topic in this paper. Some literature refers indirectly to the threat of privacy through weak data protection laws insofar as contact tracing apps are concerned, see, for example, Sihombing AK & Bratajaya Y, Contact tracing apps in ASEAN: a threat to privacy and personal data. *Kathmandu School of Law Review* 8(1), 2020, pp. 50–76. https://doi.org/10.46985/kslr.v8i1.2128.

2 Digitalisation, digital health surveillance using mobile contact tracing apps and privacy attitudes: the Singapore social and political contexts and emerging landscape

2.1 Population surveillance and the rise of 'smart nation' through digitalisation

Prior to independence from British colonial rule in 1957, Singapore had been recognised as an important hub for disease surveillance within a larger international health network (Hoo 2024). Given its small geographical space with high population density and an extensive surveillance network, such as CCTVs on roads, housing and transport networks, there is greater population control within public spaces, supported by a range of laws governing public order and online activities (Hoo 2024). Common digital health solutions during the pandemic included remote clinical consultations, health promotion through encouraging digital literacy and behaviours and surveillance and documentation of vaccination status (Ndayishimiye *et al.* 2023). The key players within Singapore's government sector are the Ministry of Health (MOH), MOH Holdings, the Office for Healthcare Transformation, the National Research Foundation and the Singapore Economic Development Board. They are supported by key research partners such as the Agency for Science, Technology and Research and the Health Technologies Consortium, which focus on artificial intelligence, telemedicine, mobile health apps and digitalisation.

It has been suggested that the combination of rapid advancements in 'smart nation' and a moral mandate in public health that supports surveillance through 'combatting Covid-19 together' has deprioritised privacy and data protection concerns in the early stages of the pandemic (Hoo 2024). Consequently, in containment efforts against Covid-19, surveillance through CCTVs and other tracking technologies is touted as protecting public safety and preventing further spread of the virus (Hoo 2024). Singapore was the first country in the world to introduce a Covid-19-related digital contact tracing app, TraceTogether, on 20 March 2020 (O'Connell *et al.* 2021). Given the high internet penetration across the island nation, harnessing the power of digital contact tracing made sense. TraceTogether was developed by the Singapore's Government Technology Agency, or GovTech (GovTech 2020). GovTech is the digital transformation agency for Singapore, tasked with mobilising the benefits of digitalisation for Singaporeans and assisting public sector agencies in their digital transformation, including developing and delivering apps, software development tools and digital services (GovTech 2020). This approach is part of Singapore's Smart Nation Initiative, which was developed in 2014 and aimed at realising the benefits of technological advancements for the population, economy and government across all sectors, from health, transport and the economy to businesses and government services (GovTech 2020; Smart Nation 2025). The Smart Nation Initiative consists of public and private partnerships, but with government oversight through cabinet ministers, highlighting a 'high degree of centrali[s]ation in the government administration' in governing public health measures (Lim 2024). The creation process for TraceTogether, which is situated within a broadly pro-innovation environment, reflected a hands-on governmental approach to protecting population health rather than delegating the responsibility to private companies. In encouraging adoption of the app, TraceTogether was promoted as a community-driven contact tracing method (GovTech 2020).

Surveillance is normalised in the population that sets the tone for relations between the government and the population in Singapore. There is strong government appetite for digital health and a drive for digital health development, creating an environment where innovations are encouraged to flourish so that they then contribute to economic benefits. The development of digital contact tracing apps and the push for nationwide use are not unusual, given the sustained, broader digitisation efforts in Singapore, which are encouraged by a centralised political leadership. The next section demonstrates an attempt to balance the practical dilemmas of protecting public and economic interests and respecting individual privacy for collected contact tracing data.

2.2 TraceTogether and privacy concerns

TraceTogether was rolled out less than three months after the first Covid-19 case was reported in Singapore in January 2020 (SMU 2022). TraceTogether utilises Bluetooth signal exchanges between mobile phones that are in close proximity to identify potential close contacts who test positive for Covid-19 (Lim 2024). A study that examined privacy technologies in TraceTogether found that user data, including phone numbers, are stored and managed jointly by the government and Google, resulting in the possibility that the geolocation data of users could be tracked by Google (Leith and Farrell 2020). The study authors similarly found that the reversible encryption feature rendered app data susceptible to disclosure (Leith and Farrell 2020). Its uptake was recorded at 25 per cent of the population in June 2020, which was considered low compared to the desired 75 per cent adoption to achieve efficacy (SMU 2022). This prompted the government to mandate its use in October 2020. TraceTogether and SafeEntry, a mandatory digital check-in system for entry into places, were complementary in contact tracing. People entering or exiting any public places or buildings were required to check in and out using the system that was mandated by law upon all businesses as part of pandemic surveillance measures (Goggin and Zhuang 2023; Lim 2024). Government proposals for developing and implementing wearables for contact tracing reportedly attracted public petitions opposing their use, signalling growing concerns about data privacy through geolocation tracking (Lee and Lee 2020; ODonnell 2020). The government responded by clarifying the use of Bluetooth technology in the wearables, where data are deleted after twenty-five days, further underscoring the difficulty in balancing the protection of public health and respecting individual privacy (Lee and Lee 2020; ODonnell 2020).

News reporting revealed concerns regarding the security of collected data in TraceTogether and the potential use of personal data for state surveillance as some of the reasons for the hesitance among the population in using TraceTogether (Sim and Lim 2020). Such concerns were said to have originated from previous experiences with data breaches in Singapore and a lack of trust regarding how gathered data could be used (Sim and Lim 2020). Additionally, it was revealed that, as part of the updates and refinement to the app, tech companies such as Google and Apple were consulted (Sim and Lim 2020), although it was unclear to the extent of the latter's input in the final app version and the control over gathered data. The government reportedly considered introducing tokens in addition to the app, however, this was met with public objections (Crabtree 2021) regarding privacy and spatial invasions (Chia 2021). It was not until January 2021 that it was revealed that TraceTogether could be used for criminal investigations under the Criminal Procedure Code (Chia 2021). This was despite assurances from the government that data collected from the app would be used solely for the purpose of contact tracing. The Singapore police had accessed the app for a murder investigation to make a prompt arrest; however, the TraceTogether data were unhelpful as the app was not installed on the suspect's mobile phone. This revelation prompted the public to express their dissatisfaction with the conflicting assurances regarding the use of gathered data. The Minister swiftly apologised for the error. An amendment to the law was promptly introduced in February 2021 to restrict the use of TraceTogether data to seven serious crimes only in the Covid-19 (Temporary Measures) Amendment Bill. The app's privacy statement was subsequently amended to reflect the use of gathered data for police investigations. TraceTogether was subsequently phased out on 26 April 2022; however, it has altered the lives of Singaporeans in terms of normalising living under surveillance and using digital contact tracing. It has similarly normalised the broad sharing of population health data with health agencies.

The TraceTogether example illustrates the range of social, ethical and legal issues and implications for populations arising from digital contact tracing. A survey indicated Singapore's appeal to service providers in marketing digital health solutions due to a relatively high willingness to share personal health information in return for benefits (e.g. receiving personalised health services) (MarshMcLennan 2020). Singaporeans have high trust in government (Edelman 2023), with population preference for governments to deliver digital health solutions compared to other

countries. Singapore adopted a regulatory sandbox approach for telemedicine and mobile medicine (MOH 2024) for Covid-19, which encouraged digital health innovations through partnerships with industries, while delivering safe health care to patients with an understanding of potential risks and benefits. The use of a regulatory sandbox is not new. It has been used in Japan to support emerging tech and cloud-based data to innovate its health-care sector through developing digital solutions (Raghavan *et al.* 2021). The Singapore government has created a conducive legislative environment for digital health-care tools to develop, and this allows for the MOH Licensing Experimentation and Adaptation Programme to test in a controlled environment prior to being rolled out to the community (Raghavan *et al.* 2021). Singapore's investment- and innovation-friendly approach, driven by the Smart Nation Initiative, provides an enabling setting for emerging tech tools to develop. Regulatory sandboxes allow industries the freedom to pursue innovations while the government can grant licences for their use on a case-by-case basis (Laurent *et al.* 2021). Singapore has implemented regulatory sandboxes across a range of sectors such as finance, health and energy (Laurent *et al.* 2021). The emphasis is often upon speed and flexibility within regulatory approaches, as when regulatory barriers are lifted or rules are relaxed to enable the technology to flourish (Laurent *et al.* 2021).

In summary, digital contact tracing apps present challenging determinations of legal and ethical boundaries for infection surveillance and control purposes (Gasser *et al.* 2020). Examples from across the world shed light on the use of surveillance data for purposes other than contact tracing (O'Connell *et al.* 2021). This raised broader challenges beyond privacy concerns, such as the lack of trust and behavioural profiling (Akinbi *et al.* 2021; Nguyen *et al.* 2022). In addition to security and privacy concerns, digital health tools can magnify socio-economic and health-care inequalities as not all households have access to the internet or smartphones, which is typically true in lower-income countries or within marginalised populations (Whitelaw *et al.* 2020).

2.3 Social and political influences in shaping population attitudes toward privacy

The concept of privacy ought to be understood in its social and political contexts. As indicated above, there is no recognition of the right to privacy under Singapore law (Lim Meng Suang v Attorney-General (2015) 1 SLR 26 (CA)). Additionally, it can also be inferred from the public messaging aimed at encouraging participation in TraceTogether as part of a broader public duty by the people to protect the health care systems, resulting in an acceptance and normalisation of digital surveillance (Lee and Lee 2020). A recent online YouGov survey conducted in September 2022 on 1,053 Singaporeans aged eighteen years and older regarding their level of concern for the security and privacy of personal data revealed that 83 per cent expressed concern for their data privacy (YouGov 2023). In Singapore, the government has often taken the lead in protecting Singaporeans, for example, communicating to the public through campaigns delivered via social media platforms and television or public service announcements in taking preventive measures in guarding against falling prey to financial scammers, engaging in healthy lifestyle habits, public messaging in relation to contact tracing as a community activity and the need for population co-operation and collaboration in containing the spread of Covid-19. The responsibility to protect oneself is thus seen as part of a broader joint effort. As such, privacy is understood differently in Singapore from the rights-based approach that is predominantly found in neoliberal societies. Given the social contract between Singaporeans and the government, privacy is less emphasised compared to priorities in a safe, stable government and secure economic benefits. Privacy concerns that were raised by some individuals regarding the use of contact tracing data suggest that there is a growing awareness of privacy within the population. An understanding of the attitudes toward privacy is helpful for regulators and policy-makers in negotiating the extent of incursion into rights and the use of gathered data in national contact tracing programmes. This is where considerations of proportionality, necessity and efficacy are valuable in determining the use of gathered data and communicating these expectations to the public in advance.

In reconsidering the TraceTogether episode above, it demonstrates a rising phenomenon where the public expression of concern for data privacy has resulted in greater government awareness of the need to show more accountability and transparency in relation to gathered data (Choo 2022). Further, as pandemics are likely to become more frequent, digital contact tracing is likely to become commonplace, with a greater push toward privacy erosion through digital surveillance, especially in a society that encourages control and discipline through social and political means (Lee and Lee 2020). This development indicates that legal preparedness extends to considering potential proportionate justifications for privacy incursions and how existing laws on data protection (in the absence of specific privacy laws) could be revised to address privacy concerns arising from digital contact tracing.

In comparison to Singapore's privacy landscape, Australia's experience of privacy concerns was premised on individual rights. It was reported that contact tracing data in the state of Victoria in Australia were sent for potential use by a data mining company, Palantir, raising privacy concerns as Australians were assured that collected data were used for contact tracing only, but they were not informed about other uses (Davey 2022). This prompted privacy scholars to express grave concerns regarding the handling of gathered data (Davey 2022). Based on the social and political landscape, standard privacy concerns that are premised upon individual rights and autonomy are less relevant to Singapore. As will be explained below, there is no specific privacy law in Singapore as understood in a predominantly Eurocentric discourse, but there are data protection laws which provide minimum data protection standards.

3 Exploring the extent of legal preparedness in implementing digital contact tracing for pandemic containment

The competing interests between privacy, social control and collective public health benefits highlight the importance of legal preparedness in ensuring that laws are capable of responding to competing priorities as part of broader responses to pandemics. Legal preparedness in public health has been recognised as one of the key ingredients for public health preparedness (IDLO 2023; USDHHS 2024). Prior to the development of a consensus on the definition of legal preparedness, the core elements of public health legal preparedness are identified as: laws as the authority and related implementation tools; competencies of the people in the agencies that are implementing public health laws in their legal preparedness; information available to the people in the agencies in shaping and applying public health laws; coordination of legal authorities across multiple agencies; and developing benchmarks for public health legal preparedness through a systematic planning process by reviewing laws and legal bases for coordination of responses by different agencies (Moulton *et al.* 2003). As indicated above, legal frameworks are essential in supporting public health emergencies through laws, regulations or administrative rules, and in affecting other aspects of national governments such as international agreements or multilateral obligations, as they provide the authority to act (Fidler *et al.* 2008). It has been suggested that public health legal preparedness should include functional tools, based on evidence and experience (from scientific and public health law materials and experiential knowledge), for authorities to apply effectively, as well as summaries of laws and procedural guidelines that will support the development of legal standards for achieving legal preparedness (Bernstein 2013). Other proposals include regular mapping and assessments of laws to identify gaps and solutions, strengthening national legal capacities to enable the implementation of laws and legal solutions, enhancing legal literacy among government officials, enforcement officers and society and cross-cutting capacity building among policy-makers, researchers and officials (IDLO 2023).

The gist of legal preparedness is captured in the latest definition, which incorporates the application of legal instruments to implement different aspects of public health emergency preparedness and response, where governmental agencies work together to address the complexity of the situation as it arises and to interpret relevant legal instruments, tools and standardised

operating procedures (GHSA 2023). Legal preparedness thus enables a transparent and clear process for the determination of functions and responsibilities of various actors and agencies during the pandemic through a whole-of-government approach. Laws provide the foundations for basic authority and responsibilities and relationships between different agencies, with significant decisional consequences for population health. In examining whether legal preparedness is adequate in relation to addressing public concerns about potential infringement of public power through legitimatisation of digital health surveillance, it is essential to consider the minimum standards for privacy and data protection that are applicable to contact tracing data.

3.1 Legal frameworks governing privacy, data protection and Covid-19-related laws

Key pandemic legislation includes the COVID-19 (Temporary Measures) Act (including its amendments) and the COVID-19 (Temporary Measures) (Control Orders) Regulations 2020. They provide the authority for key agencies to implement and enforce pandemic measures. The primary Covid-19 legislation is concerned with movement control and related matters to achieve public health goals of containing the spread of Covid-19. One of the key amendments to the Covid-19 (Temporary Measures) Act resulting from the revelation that TraceTogether had been accessed by police officers relates to personal contact tracing data. Section 80 of the law outlined the meaning of personal contact tracing data as

> 'entry or exit records, proximity information or other data – collected using any digital contact tracing tool or combination of digital contact tracing tools, that is part of a digital contact tracing system; and which, by itself or with other information, identifies any individual' (Section 80).

Section 82(1) highlighted the ways in which personal contact tracing data could be used by a public sector agency, particularly to facilitate contact tracing, including the administration and maintenance of the digital contact tracing system. A specific limitation is in place regarding its access and use by law enforcement agencies, police officers or public sector agencies, whereby no disclosure of personal contact tracing data is permitted for any investigations except for the seven specified criminal offences.

Although these amendments are made in response to public concern relating to the privacy of their contact tracing data, they provide an example of how legal preparedness could pre-empt the possibility of contact tracing data being used beyond contact tracing purposes and could provide justifiable limits to their use by law enforcement agencies. Legal preparedness thus requires government officers from the ministry of health and various law enforcement agencies to work together to assess and map these legal instruments and devise agreed operating procedures. Public expression of concern about their data privacy demonstrates some legal under-preparedness regarding considerations of the scope and limits of power pertaining to the use of contact tracing data. Crafting specific limitations on the use of contact tracing data can facilitate pandemic measures because there is an anticipation that ensures the encroachment of individual privacy is not more than expected.

A related but broader consideration of data privacy is data protection law in Singapore. As indicated above, while there is no specific privacy law based on human rights approaches, minimum data protection standards exist as part of facilitating international trade through cross-border data flows and enabling the processing of personal data by the private sector and businesses in Singapore. Data protection standards from Europe and North America exemplified cultural, social and political characteristics that prioritised personal liberties over other values; however, they are not necessarily the primary focus in Singapore (Chan *et al.* 2024). The Personal Data Protection Act 2012 (PDPA) of Singapore regulates the use and disclosure of personal data with the aim of protecting data from misuse and promoting a trusted environment for businesses

(Chan *et al.* 2024). The key aim of the PDPA is twofold: protect personal data and promote the economic interests of Singapore (Wong 2017, pp. 289–90). This approach suggests an interpretation that favours a less cumbersome environment for processing personal data while striving to maintain population trust in data protection (Wong 2017). Additionally, unlike other data protection regimes, the PDPA does not apply to the public sector, where the Public Sector (Governance) Act 2018 applies for the purpose of administering and delivering public services to Singaporeans. This divergence speaks to the broader prioritisation of encouraging economic investments and innovations where data protection laws are influenced by considerations of the broader economic interests of the nation while maintaining minimum protection for private individuals. It has been suggested that future reforms to data protection have to balance the freedom of information and speech with considerations of national social and economic policies and international standards (Chik 2013, p. 567). This aspect would be useful for legal preparedness considerations, with relevant social, political and economic considerations in developing a privacy regime that accommodates these priorities and evolving population concerns.

3.2 Summary of discussion

The state of legal preparedness in relation to implementing digital contact tracing can be improved. This can be done through reviewing a range of laws related to privacy and public health and the powers and scope of public authority so that they work together to pre-empt gaps in implementation. It would be beneficial to deepen an understanding of evolving privacy concerns that arise in the population, and take steps to address them. The distinct social, cultural arrangements and centralised political system, combined with considerations of national economic priorities and interests highlighted the significance of important influences in shaping legal preparedness. Yet, it is by no means an easy task to balance the competing priorities. However, policy-makers ought to be mindful of maintaining public trust through various means such as safeguarding interests in adequate expectations of privacy protection, appropriate use of gathered resources (data) and clear communication between the different agencies in government and the population in implementing digital contact tracing systems. It has been noted that public resistance and scepticism toward public health surveillance by the government remains a challenge, in addition to domestic political sentiments (Rozenshtein 2021). In the case of Singapore, a generally high level of trust among Singaporeans in the government is helpful in maintaining a mutual relationship of trust between the state and the population. This is because public trust has the potential to be a casualty in the process. Clearer communication to the public, supported by a policy that is aligned with public expectations regarding the use of gathered contact tracing data that were available to the government through mandatory laws during pandemics can support legal preparedness. The legislative response provides an assurance to individuals who expressed privacy concerns regarding the use of contact tracing data, recognising the potential harm from privacy infringement and any erosion of trust in data protection standards. However, public interest in safeguarding health care systems and economic interests is a significant consideration for policy-makers. The discussion indicated a swift response through legislation in addressing privacy concerns from TraceTogether, demonstrating efforts at maintaining population trust in mandated nationwide data gathering, which makes it challenging to make acceptable trade-offs in balancing privacy with public good. The progress toward digitalisation in all aspects of population life will inevitably raise further concerns about the preparedness of data protection frameworks and individual privacy.

4 Legal preparedness for future pandemics

An important part of preparedness entails learning from mistakes in past pandemics to improving legal preparedness for future pandemics. Strengthening regulatory systems as a

priority is an essential part of pandemic preparedness (Mukherjee and Goodman 2023). Greater prioritisation of legal preparedness grounded in accountability and responsibility in mandating the deployment of digital health technology during emergencies is essential. An accountable regulatory strategy to address the concerns and trade-offs includes reassessing laws that are created during the pandemic regarding the use or reuse of collected data. This is important given the mandatory, nationwide normalisation of digital health standardisation such as the mandatory use of digital contact tracing. The urgency in implementing digital health surveillance using TraceTogether may have resulted in inadequate oversight in certain aspects of data protection.

How can Singapore continue progressing and improving its legal preparedness? Regulatory sandboxes should continue to develop, given the continuous interest in and emphasis on technological innovations and solutions across all sectors. This approach will help pre-empt emerging and new privacy challenges and demonstrate proactive accountability in identifying potential risks and addressing pitfalls before digital innovations are implemented across societies. Privacy designs in digital contact tracing apps will continue to develop, and this provides an opportunity to revisit existing TraceTogether technology for the future development of contact tracing apps. The Singapore government, following the conclusion of the pandemic era, has published a white paper that identifies lessons learned and the way forward for preparation for future pandemics (Government of Singapore 2023). Legal preparedness was not explicitly mentioned in such terms; however, the essence of its preparedness is included with reference to the need to review legislative 'levers' or capabilities to respond to changes in dealing with public health threats (Government of Singapore 2023, p. 82). This approach recognises the importance of preparing a responsive regulatory framework to meet new challenges presented by evolving circumstances. As such, the groundwork leading to remedying any shortcomings in the pandemic can help strengthen and improve legal readiness and responses, consistent with a whole-of-government approach. Singapore has consistently enjoyed a high level of trust from the population and while previous breaches have not necessarily resulted in a decline in trust in the government, the TraceTogether event demonstrates that the population is increasingly aware of the importance of being informed and would prefer information to be available before participation in mandatory contact tracing programmes.

As digital surveillance through contact tracing apps will become more pervasive in future pandemics, privacy concerns will continue to grow. The suggestion for greater privacy-friendly technologies for contact tracing apps that use digital proximity tracing rather than GPS tracking (Yu and Carroll 2023, p. 159) could potentially achieve the aim of proportional data gathering. Another proposal relates to the use of decentralised, privacy-preserving technology (O'Connell *et al.* 2021). In tandem with changes to privacy friendly technologies, data protection laws could be revised to reflect an increasing possibility of reidentification of personal information (Yu and Carroll 2023, p. 160). This dual-pronged approach could potentially alleviate some privacy concerns surrounding contact tracing apps. In considering the TraceTogether technology that uses centralised and decentralised recall procedures, there is an opportunity to embed these privacy-friendly proposals into future apps. Principles reflecting proportionality, necessity, responsibility and responsiveness can guide the review and revision of relevant legislation, especially in demarcating the uses of gathered data.

Greater considerations of the implications of technological developments would be beneficial to policy-makers to ensure that any risks of harm to the population could be either pre-empted or minimised. For example, deliberations on trade-offs between privacy and public safety could be made as part of pandemic preparedness based on previous experiences, where they could then be incorporated into legal frameworks or other regulatory measures. An aspect of criticism toward contact tracing is its use for other purposes such as criminal investigations. The important lesson from the use of contact tracing data for Covid-19 is that while data are available, the law must be explicit and specific in its scope of use, time-specific and limited – that is, data must be removed

after the specified length of time and that legislation must be put in place to pre-empt the potential for misuse.

5 Conclusion

Digital surveillance has transformed the way the Covid-19 pandemic was managed and how people adjusted their lives accordingly. Regulatory choices typically reflect existing social, political and economic realities. Singapore's approach was possible because of its centralised leadership, strong political authority and cultural prioritisation of collective well-being over individual rights. This explains why Singapore succeeded where others did not. This also demonstrates that countries seeking to emulate Singapore's approach should first consider the particular societal and cultural perspectives in planning legal preparedness. Consequently, the extent of successes or failures of legal preparedness is influenced by social and political factors, population engagement with contact tracing apps, long-standing trust or distrust toward the government, the way in which the app is designed, who has an interest in the app, existing and negotiated rules of engagement in relation to privacy incursion, safeguards against potential misuse of gathered data, social licence to use those data and government handling of any breaches.

Acknowledgements. The author is grateful to the editorial team of the Special Issue for their feedback and support throughout the writing process. This research was made possible by a Wellcome Grant Reference No. 224856/Z, 'There is no App for this! Regulating the migration of health apps in sub-Saharan Africa'.

References

Akinbi A, Forshaw M and Blinkhorn V (2021) Contact tracing apps for the COVID-19 pandemic: a systematic literature review of challenges and future directions for neo-liberal societies. *Health Information Science & System* **9**, 1–15. https://doi.org/10.1007/s13755-021-00147-7

Amariles DR (2021) From computational indicators to law into technologies: the Internet of Things, data analytics and encoding in COVID-19 contact-tracing apps. *International Journal of Law in Context* **17**, 261–74 https://doi.org/10.1017/S174455232100032X

Austin, IP (2009) Singapore in transition: economic change and political consequences. *Journal of Asian Public Policy* **2**, 266–78. https://doi.org/10.1080/17516230903204745.

Ayala A, Brush A, Chai S, Fernandez J, Ginsbach K, Gottschalk K, Halabi S, Hosangadi D, Mapatano D, Monahan J, Moretti C, Pillinger M, Silvana Ramirez G, and Rosenfeld E (2022) Advancing legal preparedness through the global health security Agenda. *The Journal of Law, Medicine & Ethics* **50**, 200–03.

Bay J, Kek J, Tan A, Chai SH, Lai Y, Tan J and Tang AQ (2020) Blue Trace, the Technology Behind Tracetogether: BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders. Available at https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

Bernstein JA (2013) Beyond public health emergency legal preparedness: rethinking Best practices. 2012 Public Health Law Conference: Practical Approaches to Critical Challenges, 13–16.

Cetron MJ and Davies OL (1997) *Probable Tomorrows: How Science and Technology Will Transform our Lives in the Next Twenty Years*. New York: St. Martin's Press.

Chan HY, Toh HJ and Lysaght T (2024) Cross-jurisdictional data transfer in health research: stakeholder perceptions on the role of law. Asian Bioethics Review, 663–82.

Chia HK (2021) 'TraceTogether Saga: Timeline of Key Developments', 3 February. Available at https://sg.news.yahoo.com/trace-together-saga-timeline-key-developments-061432346.html

Chik WB (2013) The Singapore personal data protection act and an assessment of future trends in data privacy reform. *Computer Law & Security Review* **29**, 554–75.

Choo J (2022). The Use and Abuse of Personal Data by the PAP Government. New Naratif, June 7. https://newnaratif-com.libproxy1.nus.edu.sg/the-use-and-abuse-of-personal-data-by-the-pap-government/

Condie B and Dayton L (2020) Four AI technologies that could transform the way we live and work. *Nature (London)* **588**, S126–S128.

Crabtree J (2021) Public Health or Privacy Concern? The Debate Over Contact Tracing Apps. LKYSPP.

Davey M (2022) Victorians' Covid Contact Tracing Data Sent for Potential use by Data Mining Platform, *The Guardian*. 8 November. Available at https://www.theguardian.com/australia-news/2022/nov/09/victorians-covid-contact-tracing-data-sent-to-authority-for-potential-use-by-palantir

Driece RA, Matsoso P, da Silva Nunes T, Soliman A, Taguchi K, Tangcharoensathien V (2023) A WHO pandemic instrument: substantive provisions required to address global shortcomings. The Lancet Available at https://doi.org/10.1016/S0140-6736(23)00687-6

Edelman (2023) Edelman Trust Barometer Global Report. Available at https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf

Fidler D, Kamoie B, Pestronk RM, Baldridge P, Devlin L, Mensah GA and Doney M (2008) Assessing Laws and Legal Authorities for Public Health Emergency Legal Preparedness. Articles by Maurer Faculty. 295. https://www.repository.law.indiana.edu/facpub/295

Gasser U, Ienca M, Scheibner J, Sleigh J and Vayena E (2020) Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid. *Lancet Digital Health* **2**, e425–34 https://doi.org/10.1016/S2589-7500(20)30137-0

GHSA LP AP, Defining Legal Preparedness in the Context of Public Health Emergencies, May 2023.

Goggin G and Zhuang KV (2023) Apps, mobilities, and migration in the Covid-19 pandemic: Covid technology and the control of migrant workers in Singapore. *International Journal of Cultural Studies* **26**, 636–54.

Gostin LO (2004) Influenza pandemic preparedness: legal and ethical dimensions. *Hastings Center Report*, **34**(5), 10–1.

Government of Singapore (2023) *White Paper on Singapore's Response to COVID-19: Lessons for the next pandemic*. Available at https://www.gov.sg/article/covid-19-white-paper

GovTech (2020) *TraceTogether – behind the scenes look at its development*. Available at ∼'https://www.tech.gov.sg/media/technews/tracetogether-behind-the-scenes-look-at-its-development-process/#:∼:text = Taking%20advantage%20of%20Singapore's%20high,contact%20tracing%20with%20a%20difference.

GovTech Singapore. Available at ∼'https://www.developer.tech.gov.sg/products/categories/digital-solutions-to-address-covid-19/tracetogether/overview.html#:∼:text = To%20address%20this%2C%20GovTech's%20Government,complement%20manual%20contact%20tracing%20efforts.

GovTech Singapore (2025) About us. Available at https://www.tech.gov.sg/about-us/who-we-are/

Ho D (2022) The Pandemic Dilemma: when philosophy conflicts with public health. *Cambridge Quarterly of Healthcare Ethics* **31**, 1–3 https://doi.org/10.1017/S0963180121000414

Hogan K, Macedo B, Macha V, Barman A and Jiang X (2021) Contact tracing apps: lessons learned on privacy, autonomy, and the need for detailed and thoughtful implementation. *JMIR Medical Informatics* **9**, e27449–e27449.

Hoo L (2024) Mayhem in May: a social history of the 1957 Asian Flu epidemic in the colony of Singapore. *Journal of Southeast Asian Studies*, **55**, 292–317. https://doi.org/10.1017/S0022463424000304.

International Development Law Organization (IDLO) (2023) *Preventing Pandemics Through the Rule of Law Strengthening Countries' Legal Preparedness for Public Health Emergencies*. 19 September. Available at https://www.idlo.int/publications/preventing-pandemics-through-rule-law-strengthening-countries-legal-preparedness-public

International Federation of Red Cross and Red Crescent Societies Geneva (2023) World Disasters Report 2022: Trust, Equity and Local Action: Lessons from the COVID-19 pandemic to avert the next global crisis. 30 January. Available at https://www.ifrc.org/sites/default/files/2023-03/2022_IFRC-WDR_EN.0.pdf.pdf

Laurent B, Doganova L, Gasull C and Muniesa F (2021) The test bed Island: tech business experimentalism and exception in Singapore. *Science as Culture* **30**, 367–390. https://doi.org/10.1080/09505431.2021.1888909

Lee T and Lee H (2020). Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19. *Media International Australia* **177**, 47–60. https://doi-org.libproxy1.nus.edu.sg/10.1177/1329878X20949545 (Original work published 2020)

Leith DJ and Farrell S (2020) Coronavirus contact tracing app privacy: what data is shared by the Singapore opentrace app? In Park G ***et al.*** (eds.): *SecureComm 2020*, LNICST 335, pp. 80–96. ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2020 Springer Nature Switzerland AG 2020. https://doi.org/10.1007/978-3-030-63086-7_6

Lim A (2024) Tracing the smart virus in a smart city: a discursive analysis of Singapore's early pandemic surveillance response. *Urban Geography* **45**, 1780–98. https://doi.org/10.1080/02723638.2024.2336840.

Lund-Tønnesen J and Christensen T (2023) The dynamics of governance capacity and legitimacy: the case of a digital tracing technology during the COVID-19 pandemic. *International Public Management Journal* **26**, 126–44. https://doi.org/10.1080/10967494.2022.2112328

Maras M-H, Miranda MD and Wandt AS (2023) The use of COVID-19 contact tracing app data as evidence of a crime. *Science & Justice* **63**, 158–63

MarshMcLennan (2020) *Covid-19 makes Singapore's digital health on demand*. Available at https://www.marshmclennan.com/insights/publications/2020/august/covid-19-makes-singapore-s-digital-helath–on-demand-.html

Ministry of Health (2024) *Regulatory Sandbox*. Available at https://www.moh.gov.sg/home/our-healthcare-system/licensing-experimentation-and-adaptation-programme-(leap)—a-moh-regulatory-sandbox

Moulton D, Gottfried RN, Goodman RA, Murphy AM and Rawson RD (2003) What is public health legal prepared-ness? *Journal of Law, Medicine & Ethics* **31**(4), 672–83.

Mukherjee S and Goodman L (2023) Strengthening regulatory systems globally: a crucial step towards pandemic preparedness and response. *BMJ Glob Health* **8**, e012883. https://doi.org/10.1136/bmjgh-2023-012883

Ndayishimiye C, Lopes H and Middleton J (2023) A systematic scoping review of digital health technologies during COVID-19: a new normal in primary health care delivery. *Health Technol (Berl)* **13**, 273–84. https://doi.org/10.1007/s12553-023-00725-7.

Negreiro M (2021) The rise of digital health technologies during the pandemic. European Parliamentary Research Service Members' Research Service PE 690.548

Negri S, Bonfigli S, Cesta E and Federico GD (2024) Commentary: strengthening legal preparedness and response within the global health emergency framework: the role of the GHSA legal preparedness action package*. *Journal of Global Health Law* **1**, 88–105, Available at https://doi.org/10.4337/jghl.2024.01.05 (Accessed 18 June 2025)

Nguyen N, Lane B, Lee S, Gorman S L, Wu Y, Li A, Lu H, Elhadad N, Yin M and Meyers K (2022) A mixed methods study evaluating acceptability of a daily COVID-19 testing regimen with a mobile-app connected, at-home, rapid antigen test: implications for current and future pandemics. *PloS One* **17**, e0267766–e0267766.

O'Connell J, Abbas M, Beecham S, Buckley J, Chochlov M, Fitzgerald B, Glynn L, Johnson K, Laffey J, McNicholas B, Nuseibeh B, O'Callaghan M, O'Keeffe I, Kaavya Rekanar R, Richardson I, Simpkin A, Storni C, Tsvyatkova D, Walsh J, Welsh T and O'Keeffe D (2021) Best practice guidance for digital contact tracing apps: a cross-disciplinary review of the literature. *JMIR Mhealth Uhealth* **9**, e27753.

ODonnell L (2020) *Singapore's Contact Tracing Wearable Causes Privacy Backlash*. Woburn: Newstex.

Pratt B and Bull S (2021) Equitable data sharing in epidemics and pandemics. *BMC Medical Ethics* **22**, 136–36.

Raghavan A, Demircioglu MA, Taeihagh A (2021) Public health innovation through cloud adoption: a comparative analysis of drivers and barriers in Japan, South Korea, and Singapore. *International Journal of Environmental Research and Public Health* **18**, 334. https://doi.org/10.3390/ijerph18010334

Rozenshtein AZ (2021) Digital disease surveillance *American University Law Review* **70**, Article 1. Available at https://digitalcommons.wcl.american.edu/aulr/vol70/iss5/1

Schroeder T, Haug M and Gewald H (2022) Data privacy concerns using mHealth Apps and smart speakers: comparative interview study among mature adults. *JMIR Formative Research* **6**, e28025–e28025

Sekalala S, Dagron S, Forman L and Meier BM (2020) Analyzing the human rights impact of increased digital public health surveillance during The COVID-19 crisis. *Health and Human Rights Journal* **22**, 7–20

Sim D and Lim K (2020) 'Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?' *South China Morning Post,* 18 May. Available at https://lkyspp.nus.edu.sg/docs/default-source/ips/scmp_coronavirus-why-arent-singapore-residents-using-the-tracetogether-contact-tracing-app_180520.pdf

Skirpan MW, Yeh T and Fiesler C (2018) What's at stake: characterizing risk perceptions of emerging technologies. *ACM* 1–12.

Smart Nation Singapore (2025) Our Smart Nation Vision. Available at https://www.smartnation.gov.sg/about-smart-nation/transforming-singapore/

SMU Corporate Communications team (2022) The Singapore TraceTogether Story for COVID-19 Contact Tracing: Digital Product Management under Extreme Uncertainty. *SMU*. 8 April. Available at https://news.smu.edu.sg/news/2022/04/08/singapore-tracetogether-story-covid-19-contact-tracing

Stiftung, Bertelsmann BTI (2024) *Country Report — Singapore*. Gütersloh: Bertelsmann Stiftung.

Summers C, Griffiths F, Cave J and Panesar A (2022) Understanding the security and privacy concerns about the use of identifiable health data in the context of the COVID-19 pandemic: survey study of public attitudes toward COVID-19 and data-sharing. *JMIR Formative Research* **6**, e29337

US Department of Health and Human Services, *Legal Preparedness*. Available at ~https://www.hhs.gov/about/agencies/oga/global-health-security/legalpreparedness/index.html#:~:text = Legalpreparedness23/2/2024

Whitelaw S, Mamas MA, Topol E and Van Spall HGC (2020) Applications of digital technology in COVID-19 pandemic planning and response. *Lancet Digital Health* **2**, E435–E440 https://doi.org/10.1016/S2589-7500(20)30142-4

Wong YB, 2017. Data privacy law in Singapore: the personal data protection act 2012. *International Data Privacy Law* **7**, 287–302.

World Health Organization (2014) *Emergencies: Ten things you need to do to implement the International Health Regulations*. 26 May. Available at https://www.who.int/news-room/questions-and-answers/item/emergencies-ten-things-you-need-to-do-to-implement-the-international-health-regulations

WHO (2024) *International Health Regulations*. https://www.who.int/health-topics/international-health-regulations#tab = tab_1

World Health Organization (2025) International Health Regulations. Available at https://www.who.int/health-topics/international-health-regulations#tab = tab_3

Wykes T and Schueller S (2019) Why reviewing apps is not enough: transparency for trust (T4T) principles of responsible health app marketplaces. *Journal of Medical Internet Research* **21**, e12390–e12390.

YouGov. (2023). Level of concern about security and privacy of personal data in Singapore as of September 2022. Statista. Statista Inc. https://www-statista-com.libproxy1.nus.edu.sg/statistics/1366188/singapore-level-of-concern-for-security-and-privacy-of-personal-data/ (accessed 13 June 2025).

Yu S and Carroll F (2023) Securing privacy during a world health emergency: exploring how to create a balance between the need to save the world and people's right to privacy in Hewage C *et al.* (eds.), *Data Protection in a Post-Pandemic Society*. Switzerland AG: Springer Nature, pp. 145–67. https://doi.org/10.1007/978-3-031-34006-2_5

Cite this article: Chan HY (2026). Legal preparedness in implementing digital contact tracing apps in managing public health threats: the Singapore experience. *International Journal of Law in Context* **22**, 60–74. https://doi.org/10.1017/S1744552325100372