COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the gap for international pandemic control

Li Du, Vera Lúcia Carapeto Raposo, Meng Wang

Submitted to: JMIR mHealth and uHealth
on: August 04, 2020

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on it's website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressively prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the gap for international pandemic control

Li Du[1]; Vera Lúcia Carapeto Raposo[1] PhD; Meng Wang[1] BA

[1]University of Macau Macau MO

Corresponding Author:
Li Du
University of Macau
E32, Faculty of Law, University of Macau
Macau
MO

Abstract

As the world struggles with the new coronavirus (COVID-19) pandemic, tracking apps of various types have been adopted in many jurisdictions for combating the spread of the virus. However, even if successful in containing the virus within national boarders, these apps will not be effective as soon as international travel is resumed. The problem rests in the plurality of apps and their inability to operate in a synchronized manner, as well as the absence of an international entity with the power to coordinate and analyze the information collected by the disparate apps. The risk of creating a useless Tower of Babel of COVID-19 tracking apps is very real, endangering global health. We analyze the different models of contact tracing apps around the world, highlight legal challenges, and propose a coordinated solution to promote safe international travelling and global pandemic control.

(JMIR Preprints 04/08/2020:23194)
DOI: https://doi.org/10.2196/preprints.23194

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

COVID-19 Contact Tracing Apps: A Technologic Tower of Babel and the gap for international pandemic control

Abstract

As the world struggles with the new coronavirus (COVID-19) pandemic, contact tracing apps of various types have been adopted in many jurisdictions for combating the spread of the virus. However, even if successful in containing the virus within national borders, these apps are becoming ineffective as international travel is gradually resumed. The problem rests in the plurality of apps and their inability to operate in a synchronized manner, as well as the absence of an international entity with the power to coordinate and analyze the information collected by the disparate apps. The risk of creating a useless Tower of Babel of COVID-19 contact tracing apps is very real, endangering global health. This paper analyzes legal barriers for realizing the interoperability of contact tracing apps and emphasizes the need developing coordinated solutions to promote safe international traveling and global pandemic control.

Key words: COVID-19, contact tracing apps, privacy, public health, global health

Background

As the novel coronavirus (COVID-19) spreads worldwide, enabled by an unknown number of asymptomatic carriers, individuals continue to be at risk for potentially fatal infections. An effective method to contain the spread of the virus is tracing the movement of the confirmed and suspected COVID-19 cases, as well as their close contacts [1]. To this end, many countries have used contact tracing (CT) mobile apps for controlling the COVID-19 epidemic. The apps are based on various techniques that can provide the users with infection risk-level information specific to their communities and notify users who have been exposed to COVID-19, thus facilitating the public, social organizations, and the government to better prevent and control the epidemic [2].

With countries gradually reopen their borders for business and tourism, the effectiveness of using such apps for containing the spread of the pandemic is greatly weakened. The region-based development of CT apps, along with the distinguished data protection laws used in different countries and regions, have resulted in the disconnection between CT apps. The isolated CT apps, working as the technologic Tower of Babel, lost their abilities to trace and monitor the spread of the pandemic in cross-border travel, triggering challenges for global pandemic control while resuming international travel.

This viewpoint aims to raise the global awareness of the urgent need for establishing a data sharing and transferring mechanism at the international level. It advocates that a consistent international effort should be devoted to developing an international data sharing platform for global pandemic control, and further to remove the legal barriers that hinder the interoperability of contact tracing apps technology. All these efforts are aimed to contribute a better response to the potential next waves of COVID-19 and the future global pandemic crisis.

The region-based CT app development

COVID-19 CT apps are designed and developed at the regional level, employing various technologies [3]. Asian countries such as China, South Korea, and Singapore are among the first group world-wide to develop and use tracking measures for fighting against the COVID-19 epidemic. In China, for instance, the national government affairs service began developing the Epidemic Prevention and Health Information Code (EPHIC) after the pandemic surge in early February [4]. After a smart phone scans the EPHIC QR code, users submit their basic health status, residential addresses, and information about whether they have interacted with any confirmed or suspected COVID-19 individuals within 14 days. With the spread of the COVID-19 pandemic, CT apps have been widely used in many other countries.

Australia and New Zealand are also among the first countries that developed a national CT app. The COVIDSafe app launched by the Australian Department of Health, for example, helps state and territory health officials to identify and contact app users who have close contact with COVID-19 patients [5].

In Canada, CT apps were first developed by provincial governments and used within their own territories. For example, the ABTraceTogether app in Alberta, and the BC COVID-19 Support app in British Columbia both leverage the epidemic tracking information provided by the Canadian health department to inform users about their epidemic exposure risks. Later, the federal government developed the COVID Alert app, which help users to better understand the risk levels of their own regions, as well as harness geographic location information to inform other users as to whether they have encountered anyone infected with COVID-19 [6].

Some states in the United States (US) have developed CT apps for local residents such as the Care19 app in South Dakota and the Health Together app in Utah. Technology companies and research institutions have also taken up the challenges and jointly developed software such as the COVIDWatch app, NOVID app, and the Private kit app. Through different technical means, such as self-reporting by users, Bluetooth, or GPS position data, the apps can sense and record the contacts between app users and other users, indicating the risk of infection and archiving the data for the purpose of epidemic CT [7]. In May 2020, Google and Apple jointly developed CT technology and released application programming interfaces (APIs) that allow governments to work on developing their own CT apps. Since then more than one-fifth of states in the US have used the Google-Apple API code to develop their own CT apps. To further promote the use of CT technology, in September 2020, Google and Apple announced that they will incorporate the CT tool into the latest operating system of smartphones. This new system allows more states' public health authorities in the US to embrace the CT function while no extra burdens are required to develop their own CT apps [8].

In Europe, more than 20 European countries have developed CT apps for improving the management of COVID-19 [9]. Some of them created their own model for CT apps such as France, Norway, and Hungary, while other countries used the Google-Apple API code to develop their CT apps, for example, Germany, Netherland, and Switzerland [10]. In June 2020, the UK government announced that it abandoned a centralized CT app and adopted the new Google-Apple framework for future COVID-19 CT software development to help achieve more effective pandemic control [11]. In the beginning, CT apps were not welcomed either by the population or by the legal community in Europe, mostly due to privacy concerns and the requirements of the *General Data Protection Regulation* (GDPR). However, the second pandemic wave in Europe moderated the critics and highlighted the potential of CT's to control the progression of the virus.

The formation of the technologic Tower of Babel

These region-based CT apps are developed by using diverse techniques (see Table 1) and collect different types of data. For instance, South Korea, New Zealand, Israel, and Taiwan have apps that transmit the users' location. This technology model can allow the data subject to be identified by third parties, as the experience in South Korea has demonstrated, where the disclosure of an infected individual's location has made it possible to identify the person in question [12]. Some governments force the installation of CT apps to monitor the flow of confirmed cases and travelers, while other jurisdictions – Singapore, Austria, and France for example – allow users to voluntarily choose to install the apps; users can also decide whether or not to have their data collected (either automatically via the app, or by means of a voluntary act, such as reporting personal health information or by registering their location) [13]. Importantly, domestic and regional laws have different rules on data protection and privacy issues, which hamper the transnational data sharing and exchange.

Different jurisdictions offer different ways to protect data

Existing domestic and regional data protection regulations are applicable for protecting users' personal information, but their solutions are not always compatible (see Table 2). For instance, within the European Union (EU) apps are subject to the requirements of the GDPR [14], (and eventually to *Directive 2002/58/EC*) [15]. Data processing must comply with basilar general principles (Article 5/a-e GDPR) [16]: data must be collected in a fair way and the processing must be open to public scrutiny (principle of lawfulness, fairness and transparency); the collected data are to be used for a specific and clear purpose and change of purpose is not allowed (principle of purpose limitation); when possible, anonymized or pseudoanonymized data shall be used and measures must be taken to prevent the reidentification of the data subject (first dimension of the principle of data minimization); unnecessary information is not to be collected (second dimension of the principle of data minimization); data must be accurate and any mistake shall be easily amended (principle of accuracy); data are to be stored during a limited period of time and destroyed after that (principle of storage limitation).

In the US, although government-issued CT apps exceed the scope of the *Health Insurance Privacy and Accountability Act* (HIPAA) and *HIPAA Privacy Rule*, many CT apps developers claim that their apps will follow the requirements mandated by HIPAA when collecting, storing, and using users' data [17]. Some California-based companies further claim that their apps will also comply with the *California Consumer Protection Act* 2018 (CCPA) [18]. Even considering only these three standards (disregarding for now all the remaining potentially applicable regulations), several different solutions can be found. Many of the rights guaranteed by the GDPR are unknown in US law, such as the right of data subjects to receive their personal data in a commonly used format and to transmit it to another data controller, the right to data portability, and the right not to be subject to an adverse decision based solely on the application of artificial intelligence [19]. Moreover, the right to have one's data erased upon request, a basic right under the GDPR, it is absent from HIPAA, but for apps governed by the CCPA this right will apply, since it is established in Civil Code § 1798.105.

In Canada, CT apps developed by public health authorities are subject to the data protection of both the *Health*

Information Act (HIA) and the *Freedom of Information and Protection of Privacy Act* (FIPPA). For example, the ABTraceTogether, a CT app developed in Alberta, must adhere to privacy obligations of HIA and FIPPA, thus, the app only collects the user's non-identifying information to trace the contacts of the confirmed COVID-19 patients. In addition, based on the *Public Health Act* and HIA, provincial health departments can track contacts during the COVID-19 pandemic and are able to use the information for health system management and planning, policy development, and public health emergency analysis. Unlike the GDPR, FIPPA only applies to government institutions and the "personal information" protected is narrower than the concept of "personal data" adopted by GDPR (e.g., IP address and cookie data are not covered by FIPPA). Moreover, provisions in FIPPA regarding data process and data subject rights are much less extensive than those speculated in GDPR.

In China, the collection and processing of personal information garnered from COVID-19 tracking software is protected by laws and regulations governing personal information protection and infectious disease prevention and control, such as the *Cyber Security Law*, the *Personal Information Security Specifications*, and the *Regulations on Public Health Emergencies*. Accordingly, when acquiring and using personal information, the CT apps shall obtain consent from the users in advance. The data processor shall not intentionally disclose the personal information of the confirmed or suspected patients and the close contacts. Under the explicit authorization from users, disease prevention and control institutions and medical institutions can track high-risk populations based on information legally obtained. However, China's data protection laws and regulations are mainly focused on public security concerns while few provisions are about personal data protection [20]. Data subject rights granted by the relevant laws are much narrower compared with the provisions in GDPR.

Importantly, data protection laws are generally lacking in developing countries, and many have not promulgated privacy laws. According to the United Nations Conference on Trade and Development (UNCTAD), 19% of developing countries have no privacy legislation, and just 10% have developed a draft of their intended policies [21]. This privacy gap will bring significant legal barriers to transnational data transfer and sharing.

Some jurisdictions provide for transnational data transfer, while some others do not

Many domestic data protection regulations have already established conditions for transnational data transfer, and they are varied among jurisdictions. Consequently, cross-border communication or transmission of epidemic CT data will inevitably encounter legal challenges.

In China, for example, data must undergo an internal security assessment according to the regulations established by the state network departments before data can be transferred outside the country. Particularity, according to the *Security Assessment Measures for Cross-border Transfer of Personal Information (Draft for Comment)*, issued in 2019, network operators shall apply security assessment for cross-border transfer of personal information to the local cyberspace administrations at the provincial level before the personal information leaves China.

In the EU, the GDPR imposes strict limitations on data transfer to a third party (a country outside the European Economic Area or an international organization) to be processed (chapter V of the GDPR), as it is likely to happen in international traveling. Transference can only take place if the law applicable by the third party 'ensures an adequate level of protection', as confirmed by an 'adequacy decision' taken by the European Commission (Article 45 GDPR) or 'if the controller or processor has provided appropriate safeguards' regarding data safety, the protection of the subject's rights and the existence of adequate remedies (Article 46 GDPR). Apart from these two cases, only remain the specific (exceptional) conditions laid down in Article 49 GDPR. This restrict set of scenarios for data transfer might hamper the operationality of non-EU CT apps. CT apps used in a country whose data security protection do not meet the EU's standards, cannot obtain the infection risk information of the entering travelers from the EU member states, hence, the destination country is not able to determine whether a travelers has already been infected before entering the country or becomes infected after entry.

In some countries, data collected by CT apps are not allowed to be transferred outside the country. For example, in Australia, the *Privacy Amendment (Public Health Contact Information) Act 2020* prohibits a person from disclosing data collected by CT apps to another person outside Australia. The COVIDSafe also makes statements in the Terms of Service that all data collected by the government through the app will be kept in Australia and cannot be transferred out of the country.

At the international level, however, no mechanism enables the sharing of data essentials for pandemic control. These region-based CT apps work as the technologic Tower of Babel, operating independently and are not mutually recognized. The isolation of each app leaves a monitoring gap for international travel, which leads to the real challenges for the global pandemic control.

Minimizing the international health risks due to the technologic Tower of Babel

Possible options to destroy the technologic Tower of Babel

In April 2020, both the European Parliament [22] and the European Commission [23] called on member states to work together to fight the pandemic. The European Data Protection Board, in June 2020, released a statement on the data protection impact of the interoperability of contact tracing apps within the EU [24]. Few months later, in October 2020, an EU-wide system for interoperability was launched, and the first group of CT apps (i.e., Germany's Corona-Warn-App, Ireland's COVID tracker, and Italy's immuni) were linked to the system [25]. However, a broader consensus is required for the international community, since a common European approach will only solve the problem within the EU.

The WTO has established ethical guidelines for directing member parties the use of CT apps for the COVID-19 pandemic control [26]. More recently, the WTO Emergency Committee is also actively working on the development of public health tools that can help member states to deal with the pandemic risk as to the gradual resumption of international travel takes place [27]. These recommendations provide evidence-informed guidelines for member states in developing their policies for pandemic control. To date, however, no international instrument has been established to address conflicts of laws regarding data protection and privacy issues between member states. In this regard, we advocate that the global community should take the COVID-19 crisis as an opportunity for developing a mechanism that can facilitate the transnational sharing of data among countries during global public health emergencies. The big challenge is how to reach such agreement and how to enforce it.

Not long ago, the Global Outbreak and Response Network, under WHO, has established a global data collection and sharing platform, Go.Data, which was used in South African countries for Ebola surveillance [28]. Ideally, a similar model could be put in place for the COVID-19 pandemic, aimed to include a large array of countries, potentially all the affected ones. However, practical and legal impairments prevent this possibility. At most, we can aspire to create a platform with aggregated data (that is anonymized data), open-access so that international travelers, institutions, and governments around the world can use the data to track the trends of infected persons and inquire about the risk of epidemic infection in a country or region.

Another bold proposal is a common CT app, accepted by all countries and mandatory for international travelers, to help authorities to track the flow of potentially infected international travelers. This international CT app would fill the supervisory vacuum for international traveling, providing governments with real-time data to prevent the international spread of disease. Owning to the global citizenship obligation, international travelers should be required to install the tracing app [29]. The specific model of CT app would result from a common agreement. Governments should agree on a technological model for the app (see the different technologies in Table 1). In any case, only the data necessary to perform the specific task assigned to the app should be collected. Such data should not include biometric information of users and the data collected could only be used for monitoring epidemic risk. As Google and Apple have worked together to promote the CT technology that allows communication via Bluetooth between smartphones using iOS and Android systems, the technologic progress may provide an option for minimizing the international health risks. Based on Bluetooth and users' self-report, the common CT apps will notify the app users who have close contact with a COVID-19 app user during international travel in the past 14 days.

Reality check

The implementing any of these measures would not be easy in jurisdictions with rather stringent privacy laws. Each government has to accept a kind of common regime on data collection, data processing and data transfer, exclusively applicable to COVID-19 CT apps, as an exception to their respective national laws on privacy. This equates to a uniform privacy policy for all CT app users (see Table 3).

Nonetheless, even with the leadership of the WHO and under the menace of a global pandemic, the goal of fulfilling these measures is hard to reach. Governments will not give up easily of the power to decide which CT apps are to be used in their territory and under which laws (their own laws). Even if they accept to participate in this common project, without a global consensus on a legal framework for data collection, processing, and transfer, it is very unlikely that all countries agree in one single model of CT app (see Table 3). Moreover, issues raised by international data transfer are another real challenge for achieving the interoperability of CT apps. In particular, a recent decision made by the Court of Justice of the European Union (CJEU) indicates the legal challenges for transnational personal data transfer due to different data protection standards. In July 2020, the CJEU announced that the *US-EU Privacy Shield*, the personal data transfer arrangement between the US and EU, cannot provide sufficient data protection and, hence, it is invalid [30]. The decision will dramatically impact the personal data flows between the US and EU and will inevitably hamper the communication between CT apps used in the two jurisdictions. (see Table 3).

Conclusion

CT apps can be a powerful mechanism to handle the pandemic. However, the benefits will be lost if a patchwork system of noncommunicating apps becomes the norm. If governments and app developers do not act cooperatively and strategically, the global community will be left to navigate dozens of apps operating under different protocols, data models, and legal rules, ultimately hampering the effort to control the COVID-19 pandemic.

To reach an international instrument that regulates data transfer between different country’s CT apps is a challenging goal. The negotiation demands strong leadership and consistent efforts from the entire international community. Facing the increased risk of next COVID-19 waves due to the reopening of international travel, collaborative actions should be taken to minimize the COVID-19 spread risk in international travel and transport. The international community should start to work together in establishing a framework that enables data sharing and data transfer among different CT apps, breaking the existing technological Tower of Babel.

In spite of the existing difficulties, the goal of implementing these solutions is still worthy of pursuing, as it is for the common good for all human beings. Facing the global pandemic, the isolation of CT apps will not contain the international spread of infectious diseases but creating a useless technologic Tower of Babel. The international community should be prepared for the next global pandemic crisis.

At present, it is crucial for all of us, the global citizens, to collaborate with the common goal of establishing mechanisms that improves the current fragmentation of CT systems and enable effective global epidemic surveillance. Only time will tell if national governments will primarily protect their power and their regulations (that they feel as their sovereignty), under the price of paralyzing international traveling and ultimately jeopardize our common good. As it happened in the biblical accounts, the Tower of Babel will throw us apart.

Authors’ Contributions

Li Du and Vera Lúcia Carapeto Raposo designed the study. Meng Wang collected and analysed the data. Li Du and Vera Lúcia Carapeto Raposo wrote the manuscript.

Conflicts of Interest

None declared.

Reference:

. Chen S, Yang J, Yang W, Wang C, Bärnighausen T. COVID-19 control in China during mass population movements at New Year. Lancet 2020 Feb 24; 395: 764–766. [doi: 10.1016/s0140-6736(20)30421-9]
2. Ferretti L, Wymant C, Kendall M, Zhao LL, Nurtay A, Abeler-Dörner L, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. 2020 May 08; 368: eabb6936. [doi: 10.1126/science.abb6936]
3. Oliver N, Lepri B, Sterly H, Lambiotte R, Deletaille S, Nadai MD, et al. Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. Science Advances. 2020 June 05; 6: eabc0764. [doi: 10.1126/sciadv.abc0764]
4. Li ZJ, Chen QH, Feng LZ, Rodewald L, Xia YY, Yu HL, et al. Active case finding with case management: the key to tackling the COVID-19 pandemic. Lancet 2020 June 04; 396: 63-70. [doi: 10.1016/So140-6736(20)31278-2]
5. Australian Government Department of Health. COVIDSafe app. 2020. URL: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app?gclid=EAIaIQobChMI6-ew3_7Q6wIVVz5gCh2VnwUoEAAYAiAAEgJ6Q_D_BwE [accessed 2020-10-30]
6. Government of Canada. Introduction of COVID Alert today. 2020. URL: https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19/covid-alert.html [accessed 2020-10-30]
7. Fernandez E. Privacy and contact tracing apps - Google And Apple debate with world governments. 2020. URL: https://www.forbes.com/sites/fernandezelizabeth/2020/04/24/privacy-and-contact-tracing-appsgoogle-and-apple-debate-with-world-governments/#1e837deb4518 [accessed 2020-10-30]
8. Jee C. Apple and Google have launched coronavirus exposure notifications without an app. 2020 September 02. URL: https://www.technologyreview.com/2020/09/02/1007921/apple-and-google-have-launched-coronavirus-exposure-notifications-without-an-app/ [accessed 2020-10-30]
9. European Commission. Mobile contact tracing apps in EU Member States. 2020. URL: https://ec.europa.eu/info/live-

work-travel-eu/health/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en [accessed 2020-10-30]

10. O'Neill PH, Ryan-Mosley T, Johnson B. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. 2020 May 07. URL: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker [accessed 2020-10-30]
11. Chidambaram S, Erridge S, Kinross J, Purkayastha S. Observational study of UK mobile health apps for COVID-19. Lancet Digital Health 2020 June 24; 2: e388-e390. [doi: 10.1016/S2589-7500(20)30144-8]
12. Kim HE. Coronavirus privacy: Are South Korea's alerts too revealing? 2020 March 05. URL: https://www.bbc.com/news/world-asia-51733145 [accessed 2020-10-30]
13. Van Der Eycken D. Europe's plan for contact tracing apps against COVID-19. 2020. URL: https://www.law.kuleuven.be/citip/blog/europes-plan-for-contact-tracing-apps-against-covid-19/_[accessed 2020-10-30]
14. European Parliament and Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj [accessed 2020-10-30]
15. European Parliament and Council of the European Union. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). 2002. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058 [accessed 2020-10-30]
16. Hoofnagle CJ, Sloot B, Borgesius FZ. The European Union general data protection regulation: what it is and what it means. Information & Communications Technology Law 2019 February 10; 28: 65–98. [doi: 10.1080/13600834.2019.1573501]
17. Bradford L, Aboy M, Liddell K. COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. Journal of Law and the Biosciences 2020 May 28; 7: 1-21. [doi: 10.1093/jlb/lsaa034]
18. California Legislative Information. TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]. 2018. URL: http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter&article [accessed 2020-10-30]
19. Rothstein MA, Tovino SA. California takes the lead on data privacy law. Hastings Center Report 2019 September; 49: 4–5. [doi: 10.1002/hast.1042]
20. Feng Y. The future of China's personal data protection law: challenges and prospects. Asian Pacific Law Review 2019 August 05; 27: 62–82. [doi: 10.1080/10192557.2019.1646015]
21. UNCTAD. Data Protection and Privacy Legislation Worldwide. 2020. URL: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [accessed 2020-10-30]
22. European Parliament. EU coordinated action to combat the COVID-19 pandemic and its consequences. European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)). P9_TA(2020)0054. 2020. URL： https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf [accessed 2020-10-30]
23. European Commission. Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. 2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020H0518 [accessed 2020-10-30]
24. European Data Protection Board. Statement on the data protection impact of the interoperability of contact tracing apps. 2020. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf [accessed 2020-10-30]
25. European Commission. Coronavirus: EU interoperability gateway goes live, first contact tracing and warning apps linked to the system. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1904 [accessed 2020-10-30]
26. WHO. Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. 2020. URL: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 [accessed 2020-10-30]
27. WHO. Public health considerations while resuming international travel. 2020. URL: https://www.who.int/news-room/articles-detail/public-health-considerations-while-resuming-international-travel [accessed 2020-10-30]
28. WHO. WHO's data tool improves Ebola surveillance, contact tracing and decision making in Uganda. 2019. URL: https://www.afro.who.int/news/whos-data-tool-improves-ebola-surveillance-contact-tracing-and-decision-making-uganda [accessed 2020-10-30]
29. Stoner L, Perry L, Wadsworth D, Stoner KR, Tarrant MA. Global citizenship is key to securing global health: the role

of higher education. Preventive Medicine 2014 July; 64: 126-128. [doi: 10.1016/j.ypmed.2014.05.006]

30. Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, C-311/18. 2020. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf [accessed 2020-10-30]

31. Li JF, Guo XY. Global deployment mappings and challenges of contact-tracing apps for COVID-19. SSRN Electronic Journal. 2020 May 24. [doi: 10.2139/ssrn.3609516]

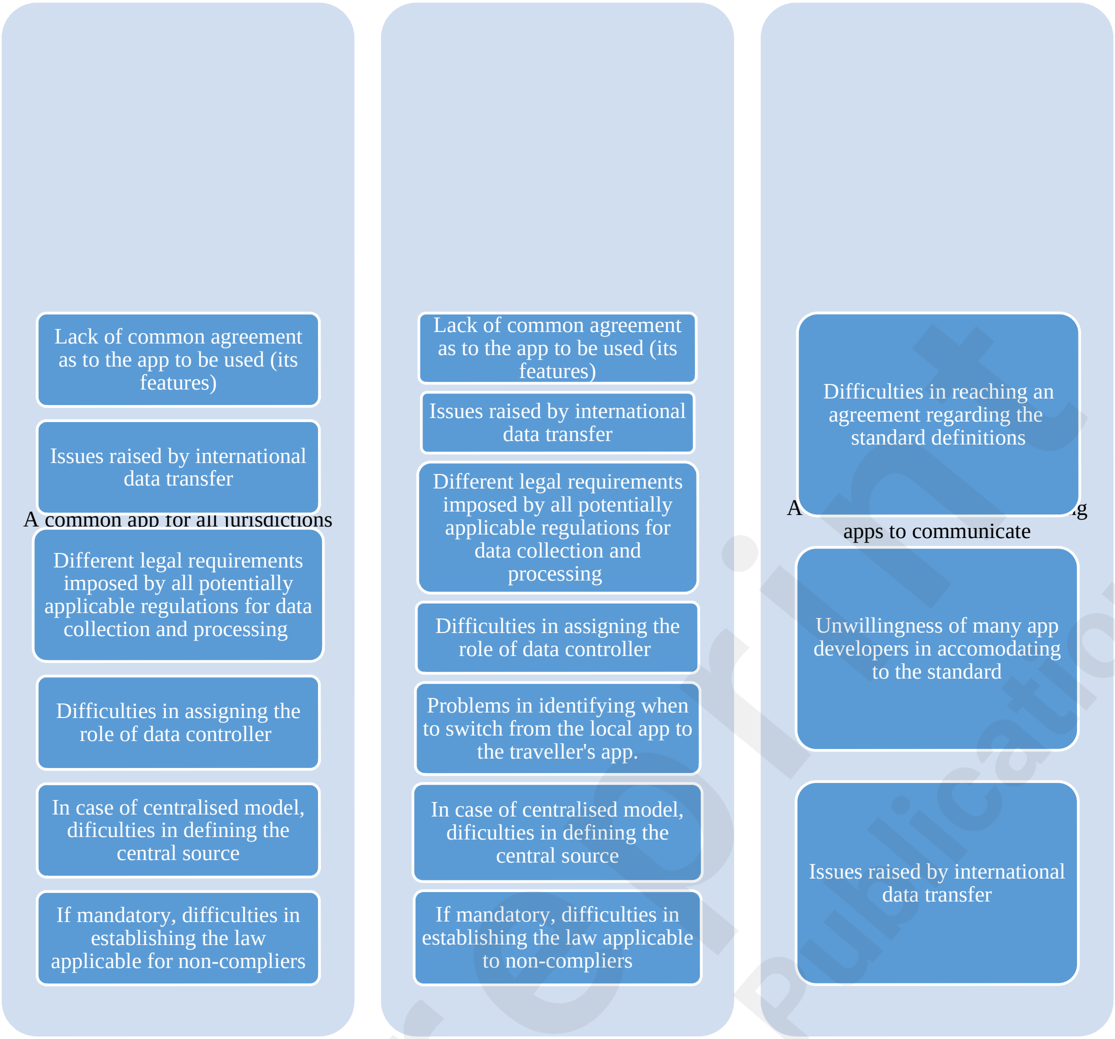
Table 1: Technologies Used in COVID-19 Contact Tracing Apps and Potential Legal Challenges

Technologies used for Contact Tracing apps*	App examples	Potential legal challenges
Tracking location by GPS	• Self-quarantine safety protection (South Korea) • Epidemic Prevention and Health Information Code (China) • National Government Service Platform (China) • HaMagen (Israel) • NZ COVID Tracer (New Zealand) • Canada COVID-19 (Canada) • ArriveCAN (Canada) • COVID Safe Paths (USA) • Healthy Together (Utah, USA) • Care19 (North Dakota, USA)	• Personal privacy issues, including the disclosure of personal privacy location information, personal health information, etc [31]. • It is not clear who will bear the responsibility if the users' location is not accurate, and if the disease condition is reported incorrectly due to the location information error, and if there is a false report. • If the state or the authorities adopt the technology on a large scale, but the technology fails due to satellite signals or technical failures, how can it be remedied? • Some software shares data with the authorities, which could make it possible for the government to access personal location information. The issue is especially sensitive when it comes to the location of people of different races. • Location can reveal a lot about a person (sexual orientation, religion, political affiliation) that is not directly related to the pandemic control. • For apps that data collected are kept in a central remote server. If attacked, there will be a massive privacy breach.
Contact tracing by GPS	• Epidemic Prevention and Health Information Code (China) • National Government Service Platform (China) • HaMagen (Israel) • NZ COVID Tracer (New Zealand) • COVID Safe Paths (USA) • Healthy Together (Utah, USA) • Care19 (North Dakota, USA)	• All legal challenges for using GPS in tracking users' location. • Using GPS for contact tracing requires analyses of the location information of multiple users by means of big data. This will involve how to properly store and use the personal information of users, and other legal issues related to personal data privacy protection.
Contact tracing by Bluetooth	• TraceTogether (Singarpore) • COVIDSafe (Australia) • Stopp Corona (Austria) • ABTraceTogether (Alberta, Canada) • ProteGO (Poland) • Corona-Warn-App (Germany) • SwissCovid (Switzerland) • HaMagen (Israel) • COVID Safe Paths (USA) • Healthy Together (Utah, USA) • Care19 (North Dakota, USA) • CovidWatch (USA) • NOVID (USA)	• Although most of the software using Bluetooth technology has claimed that they will not obtain user information, just to warn the risk of disease through distance perception, data security is a big concern as hackers may attack the Bluetooth firmware to obtain the user's personal information and location data information [31]. • Bluetooth technology is faced with many technical incompatibilities between devices, which will lead to the incomplete information collection and to some extent unable to effectively control the spread of the disease. • Privacy concerns, but when Bluetooth relies on the Bluetooth Low Energy (BLE) technology all information is stored in the user's device (decentralised system), thus raising less privacy issues.
Self-reporting by users	• Epidemic Prevention and Health Information Code (China) • National Government Service Platform (China) • Self-quarantine safety protection (South Korea) • HealthLynked COVID-19 Tracker (USA) • Relief Central COVID-19 (USA) • PatientSphere for COVID-19 (USA) • Obvio-19 (USA) • How We Feel (USA) • COVID Safe Paths (USA) • CovidWatcher (New York City, USA) • Care19 (South Dakota, USA)	• Self-reporting software usually requires users to upload their own personal data. The software will analyse the location information and personal health data of multiple users by means of big data. This will involve how to properly store and use the personal information of users, and other legal issues related to personal data privacy protection. • Under the absence of legal oversight, self-reporting of health conditions by users can lead to excessive collection of personal information by software. • Centralised data storage may lead to improper access to information and excessive dissemination of users' personal information. • Some self-reporting software shares data with the authorities, which could make it possible for the government to access personal information. • There are no careful legal regulations to govern the software and technology that collect data centrally for public health purposes in the context of such pandemics.

Table 2. Examples of domestic and regional data laws applicable to data collection and data sharing of CT apps

Countries or regions	Applicable data laws
The United States	*Health Insurance Privacy and Accountability Act (HIPAA)* *HIPAA Privacy Rule* *California Consumer Protection Act*
The European Union	*General Data Protection Regulation* *Directive 2002/58/EC*
Canada	*Health Information Act* *Freedom of Information and Protection of Privacy Act*
China	*Cyber Security Law of the People's Republic of China* *Personal Information Security Specifications*
Australia	*Privacy Amendment (Public Health Contact Information) Act*

Table 3. Potential solutions to the Tower of Babel and barriers to implementing these solutions



A common app for all jurisdictions

Lack of common agreement as to the app to be used (its features)

Issues raised by international data transfer

Different legal requirements imposed by all potentially applicable regulations for data collection and processing

Difficulties in assigning the role of data controller

In case of centralised model, dificulties in defining the central source

If mandatory, difficulties in establishing the law applicable for non-compliers

Lack of common agreement as to the app to be used (its features)

Issues raised by international data transfer

Different legal requirements imposed by all potentially applicable regulations for data collection and processing

Difficulties in assigning the role of data controller

Problems in identifying when to switch from the local app to the traveller's app.

In case of centralised model, dificulties in defining the central source

If mandatory, difficulties in establishing the law applicable to non-compliers

A g apps to communicate

Difficulties in reaching an agreement regarding the standard definitions

Unwillingness of many app developers in accomodating to the standard

Issues raised by international data transfer