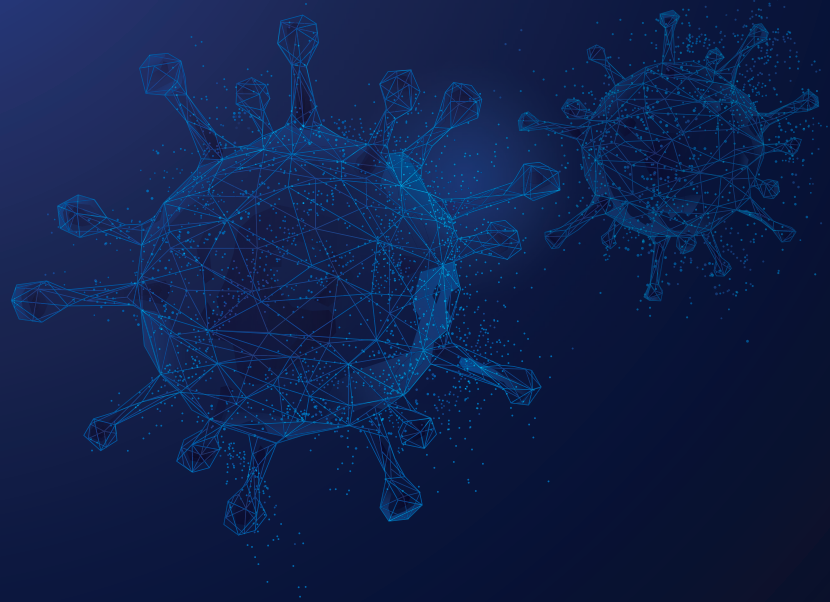
the global voice of the legal profession

International Bar Association

Covid-19 pandemic

Communications Law Committee survey responses



IBA Communications Law – Covid-19 survey responses

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
Australia	In April 2020, the Australian Government released the COVIDSafe app. Download and use of the COVIDSafe app is voluntary. When a person registers for the app they will be asked to provide a name (which may be a pseudonym), age range, phone number and postcode. The COVIDSafe app uses Bluetooth to look for other devices that have the app installed. It records when a 'contact' occurs, which is that a user is within approximately 1.5 metres of another user of the COVIDSafe app for 15 minutes or longer. The contact information is encrypted and stored on the user's device for 21 days, after which it is automatically deleted. The app does not track location. If a COVIDSafe app user tests positive for Covid-19, a health official will obtain that person's consent to upload their app data to the National COVIDSafe Data Store (the central repository of all uploaded tracing data). If consent is not obtained, then the data cannot be uploaded. If data is uploaded, health officials (but no-one else) will use the data to contact those other users of the COVIDSafe app who have come into contact with the person. Unlike tracing apps introduced in some other jurisdictions, the COVIDSafe app does not use the tracing API developed by Google and Apple.	No pre-existing laws have been used to electronically track citizens. Specific regulation was required to authorise the COVIDSafe app and the use of that data. Monitoring of citizens in quarantine is undertaken via physical means, rather than electronic tracking (in particular, requirements to remain in hotel quarantine and checks by police on in-community quarantine arrangements).	Initially the COVIDSafe app was authorised under the Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements – Public Health Contact Information) Determination 2020 (Cth). This was a regulation put in place under Australia's Biosecurity Act 2015 and was a temporary measure until Australia's Privacy Act 1988 could be amended to regulate the COVIDSafe app. In May 2020, the Privacy Act was amended to impose significant protections for COVIDSafe app data collection and use well beyond the protections usually afforded to personal information, including health information, under the Privacy Act. Broadly: 1. COVIDSafe app data may only be collected and subsequently used with the consent of the individual. It may only be used and disclosed for contact tracing activities and for the proper functioning, integrity and security of the COVIDSafe app and the National COVIDSafe Data Store. 2. The existing mandatory data breach notification regime in the Privacy Act will apply, with all data breaches involving COVIDSafe data considered to be serious breaches that are required to be notified to the Australian Information Commissioner and may also be required to be notified to affected individuals. 3. The data held in the National COVIDSafe Data Store must be held in Australia (and a breach of this requirement is a criminal offence). When the COVIDSafe app ceases to be used, all the data held in the National COVIDSafe Data Store must be destroyed. 4. Unauthorised collection, use or disclosure of COVIDSafe app data or requiring a person to use the app (eg, employers requiring employees to use it) are criminal offences. Other offences include decrypting COVIDSafe app data held on a device. 5. The Australian Privacy Commissioner may take action if the requirements relating to collection and use of the COVIDSafe data are breached and the police may also take action. Most Australian States and Territories have their own separate privacy laws. To the extent that personal information is obtained by a State or Territory health authority in relation to any form of contact tracing, it would need to also comply with that State or Territory legislation (if it were applicable).
Belgium	Yes, in particular: ▪ The Belgian Government (see sponsor logos at the bottom of the Coronalert website available at https://coronalert.be/en/); ▪ the Walloon, Brussels and Flanders regions (see here and here).	▪ No use of existing laws. Rather, enactment of special laws and Royal Decrees. ▪ Law of 27 March 2020 empowering the King to take measures to combat the spread of the coronavirus Covid-19 (II), Articles 2, 5, section 1, (1) and (6) (available here). ▪ Royal Decree of 17 September 2020, implementing Royal Decree No 44 of 26 June 2020 (available	The Belgian Data Protection Authority (DPA) published several opinions on the proposed draft royal decrees/laws enabling the tracking of citizens via contact tracing apps. In its opinions, the DPA rejected the first proposed royal decrees/laws in the light of the GDPR and the Belgian law implementing GDPR (law of 30 July 2018 on the protection of individuals with regard to the processing of personal data). All opinions are available here: www.autoriteprotectiondonnees.be/citoyen/themes/covid-19.

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
		here) concerning the joint processing of data by Sciensano and the contact centres designated by the competent regional authorities or by the competent agencies, by health inspections and by mobile teams in the context of contact follow-up with (presumed) persons infected with the coronavirus Covid-19 on the basis of a database at Sciensano, MB, 17 September 2020, p 66960. (source here). The deployment of the Belgian digital application 'CoronAlert' requires two cooperation agreements between the federal state and the federated entities: (i) a legislative agreement defining the legal framework for the joint processing of data by Sciensano, contact tracing centres, health inspectorates and mobile teams, and (ii) an enforcement cooperation agreement setting out the rules for digital contact tracing. However, neither of these two texts is ready yet. In the meantime, the government has developed an interim regulation for the use of the digital contact tracing application. The Royal Decree deals mainly with the technical side of the application, including its functionalities and operations, technical specifications and interoperability, as well as the information obligations incumbent on its developers and managers. But the text also includes control measures. The operation of the application and its necessity will be regularly controlled, evaluated and rectified under the impetus of the Interfederal Testing and Tracing Committee. The application will also be subject to an information security audit. Source here.	The DPA also stressed that contact tracing apps must comply with the rules and guidelines issued by the EDPB, in its Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the Covid-19 outbreak. It has also published Q&As on the topic (See here).
Bulgaria	Bulgaria has not sponsored tracing apps tracking Covid-19; however, there is such an app already in use. In April 2020, a private company, ScaleFocus, developed a Covid-19 specific app – ViruSafe. Such app has been provided to the Ministry of Health for free and is intended for use by Bulgarian citizens. The app was presented to the public on 4 April 2020 and launched for mass use on the Google Play and AppStore on 7 April 2020. The app was officially	Bulgarian Parliament approved amendments to the Law on Electronic Communications effective as of 24 March 2020 and affecting data retention and data disclosure obligations of the electronic communications services (ECS) providers, and more specifically: ▪ ECS providers were made subject to the obligation to retain traffic data for the needs of enforcing mandatory isolation and in-hospital treatment of sick individuals and carriers of the	Bulgarian DPA has not issued guidelines, recommendations, or other relevant regulations in respect of the ViruSafe app. A case seeking the abolishment of the controversial new data traffic obligations was brought before the Bulgarian Constitutional Court. In its decision of 17 November 2020, the latter court announced the provisions of the Law on Electronic Communications dealing with the newly imposed data retention and data disclosure obligations of the ECS providers as contradictory to the Bulgarian Constitution because they were non-proportional and contradictory to the general constitutional

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	recognised as governmental tool in the fight against Covid-19 at the end of May, when by virtue of Order RD-01—284, dated 29 May 2020, the Minister of Health introduced the National Information System for Combatting Covid-19. Said order mentions the mobile application as a module of the National Information System for Combatting Covid-19, which, after entering more than two symptoms, generates an e-mail to the respective general practitioner responsible for the health insured individual and up-to-date information about the respective person would be sent. Pursuant to the description of the app available in Google Play and AppStore, however, ViruSafe has more features, including daily symptoms log and health status tracker, as well as location tracker, used to create a heatmap with potentially infected people. Although ViruSafe has been mentioned as a module of the National Information System for Combatting Covid-19, the app and processing of the information gathered by the app have not been regulated by explicit statutory rules. Currently there is no public information about the use of the app either.	disease, that have refused or do not comply with the mandatory isolation or treatment. ▪ The heads of the Chief Directorate National Police, Capital Directorate for Interior Affairs and the regional directorates of the Ministry of Internal Affairs are now authorised to request disclosure of traffic data. ▪ The procedure provides for immediate access without court order, based solely on the request of the head of the respective authority. Following the disclosure, the requesting authority must notify the competent court for the disclosure request. Should the court assess the request as unlawful, the requesting authority must destroy the disclosed data in 24 hours and notify the ECS provider. ▪ The new obligation is in effect until the end of the necessity for enforcement of the mandatory isolation and hospital treatment of the relevant individuals. Through additional legislative amendments, the obligation has become a generally applicable statutory rule (effect even beyond the term of the emergency situation). Currently there is no public information if the Ministry of Internal Affairs has used its new powers or how often the new powers have been exercised.	principles protecting privacy. As of the date of the above-referred decision of the Bulgarian Constitutional Court those provisions are not applicable anymore.
Chile	Yes	No	The only official tracing app in Chile is ‘CoronApp’, a centralised app using GPS technology. Its privacy policy covers issues such as the purpose of processing personal information, the way in which data is stored, access by third parties and the exercise of rights of access and rectification by the data subject, among others. The drafting of the policy has been criticised, based on: ▪ Lack of a clear legal basis. Chilean law provides only for two legal bases: legal authorisation and consent. However, the policy refers to the powers of the Ministry of Health (MINSAL) conferred by law but, at the same time, requires consent as a condition for the use of the app. A clear definition of the legal basis would have requested consent only for the processing that does not fall within MINSAL’s powers. ▪ Users can add the sensitive information of third parties, the ‘dependent users’, who do not grant consent or may not even know that their health data is being gathered. ▪ The purpose for which the data is stored and processed is broad, with no further specification as to ‘the protection of public health’. This is relevant since, according to our legislation, data provided under the consent rule can only be

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
			used 'for the purposes for which it was collected'. It is not clear whether the main functionalities satisfy the stated purpose and whether the personal data that is requested satisfy such purposes. ▪ The policy only refers to rights to access, update or correct the personal information but does not refer to rights of deletion. ▪ Finally, the application offers the possibility of delivering alerts on high-risk situations, a mechanism that can be misused or abused, considering that it is based on the user's voluntary declaration. It is not clear what are the parameters that the authority will use to determine whether it will carry out control actions.
Denmark	Yes. The app Smittestop, which was first made available to the public on 18 June 2020, is a public/state-sponsored app. The app is administered by the Danish Patient Safety Authority (DPSA –in Danish, *Styrelsen for Patientsikkerhed*), according to Executive Order No 896 of 17 June 2020 (EOS) under section 21(b) of the Danish Epidemic Diseases' Act (DEDA – in Danish, *Epidemiloven*), which the Danish Parliament passed on 17 March 2020 in direct response to the outbreak of Covid-19 and the prospects of creating a state-sponsored tracing app. On a technology-related level, the app is based on Bluetooth technology, particularly the Privacy-Preserving Contact Tracing Framework API (Application Programming Interface) provided by Apple and Google. Therefore, user registration on and utilisation of the app is required for it to serve its purpose, and the Danish Patient Safety Authority does not automatically input whether a user is infected with Covid-19.	Yes. At the onset of the rapid spread of Covid-19 in Denmark, the Danish Ministry of Foreign Affairs (DMFA) stated that it was using localisation data from mobile phones to trace Danish citizens abroad with the purpose of (a) advising them to return to Denmark immediately, and (b) to plan their departure from their respective location abroad. In practice, the DMFA did not (according to the information that is publicly available) process the information itself but relied on Danish mobile providers to send out messages to Danish mobile users abroad. Further, before making Smittestop available to the public, the Danish research institute, Statens Serum Institut (SSI) informed that it had requested and received anonymised/aggregated mobile phone data from Danish telecommunication providers to track the effects of for example social distancing measures introduced by the Danish government. However, as described in responses to further questions, it is questionable whether these requests were justified within the legal framework existing at the time.	**Smittestop** The Danish Data Protection Agency and the Danish Data Protection Board have been involved in the development and ongoing evaluation of Smittestop, as the processing of personal data through the app falls within the scope of various regulations within data protection. Besides the GDPR (General Data Protection Regulation), this includes (a) the Danish Data Protection Act (DDPA – in Danish, *Databeskyttelsesloven*), and (b) Executive Order No 1148 of 9 December 2011 (EOOC – in Danish, *Cookiebekendtgørelsen*). The app is not based on telecommunications data, that is, localisation data, as specified in the ePrivacy directive; it seems that the app does not give rise to any concerns in this relation. The connection between the rules mentioned above and DEDA/EOS is that the general regulations regarding data protection require specific user consent under Article 4(11) and 7 of the GDPR and the EOOC, whereas the remaining data processing, carried out in connection with the operation, and EOS regulates the app's use. The data processing taking place during the app's use is naturally required to be compliant with the GDPR and DDPA. Therefore, EOS contains provisions regarding: ▪ the data controller: according to section 1(1) the DPSA is the data controller; ▪ the data processing purpose: is to preclude and prevent the spread and transmission of Covid-19. In this connection, the app aims to contribute to diminishing trains of infection transmissions by enabling users to receive an electronic notification that they have been in contact with other infected users of the app, *cf* EOS section 1(2); and ▪ data processing limitations: according to EOS s 1(4), the DPSA may not process personal data for purposes other than those specified in EOS section 1(2). In addition, EOS distinguishes between (i) data processed by Danish health authorities, and (ii) data processed on the user's phone. In this respect, EOS contains provisions regarding categories of personal data processed, transferral and disclosure of personal data from/to third parties, and deletion of personal data.

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
			Based on the above-mentioned, Smittestop and its specific regulation (ie, EOS), are seemingly compliant with the GDPR, DDPA and guidance from the Danish Data Protection Agency. **The DMFA's request and use of telecommunications data** The DMFA's request for disclosure of telecommunications data gives rise two main considerations: Firstly, whether and to what extent the telecommunications provider may store and process this location information. Danish telecommunication providers' processing of localisation data is governed by the ePrivacy Directive, which has been implemented into Danish law in Executive Order No 715 of 23 June 2011, (EOEP – in Danish, *Udbudsbekendtgørelsen*). Under the EOEP, the use of localisation data is very restricted. Secondly, whether and to what extent this data may be transferred to third parties such as the Danish authorities. The above-mentioned does not give Danish telecommunications providers' access to transfer localisation data to third parties, including Danish authorities, unless the third party uses said data to provide the value-added service on behalf of the provider. According to Article 15 of the ePrivacy Directive, the Member States may adopt legislative measures to restrict the providers' obligations found within EOEP section 24, when such restrictions constitute a necessary, appropriate and proportionate measure related to national or public security. Previously, no such measures have been implemented in the EOEP or otherwise in Danish law. However, in connection with the spread of Covid-19, the Danish parliament adopted Executive Order No 216 of 17 March 2020 with reference to DEDA. In this, it is stated that all legal persons must, at the request of the DPSA or the police, provide relevant information, including '[…] information that may serve to locate an end-user in connection with his use of electronic communication networks or services.' Said Executive Order is no longer in effect. No formal decisions or assessments have been made as to whether the use of localisation data was in accordance with Danish law. **SSI's request and use of telecommunications data** According to the European Data Protection Board's guidelines 04/2020, anonymisation refers to using a set of techniques to remove the ability to link the data with an identified or identifiable natural person against any 'reasonable' effort. Although the actual effects and adequacy of the anonymisation implemented might be questionable, the data requested by and provided to SSI should most likely be considered as aggregated anonymised data, which may be stored. No formal decisions or assessments have been made as to whether the transferal of data to SSI was in accordance with Danish law.

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
Finland	Yes, it will be ready and available soon.	No, the privacy laws in Finland are rather strict with these issues.	Tracking applications are solely decided by users and with anonymity so there is no mechanism in place for tracing people and identifying persons, the application will send you information when consented about eventual exposure of virus infected.
Ghana	Yes	No	In the early stages of the launch of the GH Covid-19 Tracker, it was noticed that app collected more information than it relevantly needs (data minimality). Secondly the information was not validated – especially the phone number which means one can make entries on behalf of others and creates integrity issues with the data collected (data quality). There were no direct recommendations from the Data Protection Commission concerning the use of the App for collecting personal data for the purposes of Covid19 tracking. However, public concerns caused the App to undergo some modifications to address the pending issues raised above.
Italy	The Italian government, in cooperation with the private tech company Bending Spoons SpA, has developed and promoted 'Immuni', an app available for Apple and Android portable devices (see here). Immuni aims at notifying users being potentially exposed to the virus, even when they are asymptomatic. According to Immuni privacy policy, the app uses Bluetooth Low Energy technology and does not collect any data that would identify the user (including data on his/her identity or location). For the sake of completeness, there are also some apps which have been developed or promoted at the regional level: they generally do not track Covid-19 infections but aim at monitoring the spread of Covid-19 or assist patients under quarantine. For example, the Lombardy administration has improved the app 'AllertaLOM' (see here) – already used to send notices in case of emergency situations – by adding a survey which can be filled in by users to collect from them anonymous information on their habits and health status. This would allow to monitor and map the spread of Covid-19. In addition, the Trentino administration activated the app 'TreCovid19', which offers official information and updates on the matter and helps the remote monitoring and assistance of patients under quarantine.	At present, no laws (including telecommunications laws) have been used in Italy to track citizens who are infected and ensure that they are in quarantine. Police forces generally monitor the compliance with quarantine requirements according to national and local laws (eg, through verifications on-site or on the road, or by calling the persons on their landline or mobile numbers). At present, the only contact tracing system specifically established at the national level is the Immuni app. Pursuant to Article 6 of Decree-Law No 28 of 30 April 2020, the only tracking activity conducted by the app aims at alerting people who could have come into contact with people tested positive with Covid-19, in order to prevent contagion.	The Data Protection Authority acknowledged that the right to privacy could be limited – to some extent – in light of the current Covid-19 emergency, provided that the relevant restrictive measures are adopted on a temporary basis and comply with general principles on data protection. With respect to tracking activities, the Authority recommended to comply, in general, with the following: 1. The requirements established under Directive 2002/58/CE ('e-privacy Directive'), which allows the use of localisation data in case they are anonymous or upon the data subject's consent. 2. The adoption of specific national laws allowing the relevant activities, for example, for public health and security reasons and establishing the appropriate security measures aiming at protecting the data subjects' privacy. 3. The data controller should favour the use of anonymous or aggregate data (or, in any case, tools which are less invasive than apps tracking data subjects); if it is not possible, appropriate safeguards should be adopted. 4. General principles on data protection should be complied with (in particular: proportionality, necessity, minimisation, purpose limitation and transparency principles); the data collected should also be deleted as soon as they have been used and any re-use should be prohibited. 5. A data protection impact assessment should be generally carried out. 6. It is not possible to impose the obligation to install the Immuni app (as other apps developed or promoted by public entities) and failure to install them should not imply any negative consequence for data subjects. For the sake of completeness, a specific decision has been issued by the Italian Data Protection Authority to authorise data processing activities carried out through the Immuni App (Decision No 95 of 1 June 2020), provided that certain requirements

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	According to non-official information available online, the Veneto region is also developing a specific app for its citizens.		were met (in particular, in terms of information to be provided to the data subjects and other technical safeguards).
Netherlands	On 10 October 2020, the Dutch government launched the CoronaMelder ('Corona-Notifier') app. The app is meant to assist with the contact-tracing efforts undertaken by the local health authorities (*Gemeentelijke GezondheidsDienst* or GGD). The app is provided for by an explicit legal ground included in the Covid-19 legislation which was adopted on 10 October. This legislation is temporary and must be renewed every three months.	The government explored using telecommunication (ie, location/triangulation) data from telecom providers to increase its visibility on aggregated mobility during (partial) lockdowns but needed to amend the Dutch Telecommunications Act (*Telecommunicatiewet*) to do so. After seeking advice from the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), the government has shelved these plans for the time being. It is worth noting that the advice from the DPA identified some significant risks in the proposal and that it was possible to (re)identify individuals or groups of individuals. Currently, the government only relies on aggregated mobility data derived from already existing sources, including railway and other public transport operators, traffic metrics (number of cars on the road) and mobility data published by parties such as Google.	From the onset, the Dutch DPA has been quite vocal and involved with the various proposals, and published guidance around Covid-19 related topics, such as the processing of telecommunications data to track mobility and the development of the Covid-19 app. Other topics on which it published include the processing of health data, temperature checks, private Covid-19 tests and good practices for remote working and education. **Covid-19 app** One of the reasons the Covid-19 app has a legal ground specifically provided for by law, is because the DPA believed this was required to ensure the app met the requirements of the GDPR as well as the Dutch Implementing Act GDPR (*Uitvoeringswet AVG*). **Processing of telecommunication data** As mentioned above, the DPA provided legal advice to the Dutch government in relation to its proposed changes of the Dutch Telecommunications Act.
Singapore	Yes – a 'TraceTogether Programme' has been developed by the Ministry of Health (MOH) and Government Technology Agency (GovTech) of Singapore. The TraceTogether Programme includes the TraceTogether App and the TraceTogether Token – see further responses. TraceTogether is built on the BlueTrace protocol, designed by the Government Digital Services team at GovTech. Mobile apps and wearables that deploy the BlueTrace protocol blend decentralised and centralised models of contact tracing. The collection and logging of encounter/proximity data between devices that implement BlueTrace is done in a peer-to-peer, decentralised fashion, to preserve privacy. At the same time, the analysis and the provision of epidemic control guidance is done centrally by a trusted public health authority. For transparency, the BlueTrace protocol and OpenTrace reference implementation have been made available publicly on GitHub at: https://github.com/OpenTrace-Community.	Under the Infectious Diseases (COVID-19 – Stay Orders) Regulations 2020 ('Regulations') issued under the Infectious Diseases Act (Cap 137): ▪ the authorities may order any 'at-risk individual', who has been issued with a quarantine order under the Regulations, to do one or more of the following, during the period that the quarantine order applies to the at-risk individual under the Regulations, to enable the electronic monitoring of the at-risk individual's whereabouts at any time during that period: (a) to wear in the specified manner and keep activated at all times the electronic wristband provided by the specified person; (b) to use a mobile application in the manner specified in the order; (c) to ensure that the electronic gateway device provided by the specified person is at all times activated at the at-risk individual's place of accommodation; and	The Personal Data Protection Act 2012 (PDPA) regulates the collection, use and disclosure of personal data in Singapore. **Private organisations and individuals** The data protection regulator in Singapore, the Personal Data Protection Commission (PDPC), has published an advisory stating (inter alia) that: ▪ organisations may collect personal data of visitors to premises for purposes of contact tracing and other response measures in the event of an emergency, such as during the outbreak of the coronavirus disease 2019 (Covid-19); ▪ in the event of a Covid-19 case, relevant personal data can be collected, used and disclosed without consent during this period to carry out contact tracing and other response measures, as this is necessary to respond to an emergency that threatens the life, health or safety of other individuals; and ▪ as organisations may require national identification numbers to accurately identify individuals in the event of a Covid-19 case, organisations may collect visitors' National Registration Identification Card (NRIC), Foreign Identification Number (FIN) or passport numbers for this purpose. However, the PDPC also clarified that organisations that collect personal data for establishing Covid response measures must comply with the Data Protection Provisions of the PDPA, such as making reasonable security arrangements to protect the personal data in their possession from unauthorised access or disclosure

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	TraceTogether App The TraceTogether App is a mobile application, for voluntary download, developed to support existing nationwide efforts to combat Covid-19, by enabling community-driven contact tracing. The app is designed to run in the background on iOS and Android smartphones and, when phones running the app are detected to be in proximity with each other, using the Bluetooth protocol, they log a temporary ID to record the 'contact'. This information is stored securely on the phone. If a user tests positive for Covid-19, the user can choose to allow MOH to access the data in the app to help identify close contacts. These contacts will be contacted via the app by the MOH, who can in turn then decide whether to grant consent to upload their TraceTogether data to MOH. Additional details: ▪ Geolocation data is not collected (ie, the information retrieved will not be able to identify where the user had been in Singapore). User personal information, including their unique identification number and mobile number, is not revealed to other TraceTogether users. Rather, they are substituted by a random permanent ID. This information is stored in a secured server. ▪ As an added layer of protection, TraceTogether also creates temporary IDs that change regularly. Only these temporary IDs are exchanged between phones. These measures seek to protect users from malicious actors who may seek to eavesdrop and track interactions over time. ▪ In addition, the Bluetooth information stored on the phones is automatically deleted after 25 days. Users may also specifically request for identification data to be deleted on the servers unless proximity data has already been uploaded as a confirmed case. Upon such request, the Government will delete the user's mobile number, identification details and User ID from the server. This renders meaningless all data that the user's phone has exchanged with other phones, because such data will no longer be associated with the user.	(d) to do such other things as may be specified in the order that is incidental to sub-paragraph (a), (b) or (c). ▪ Any person who unlawfully destroys, damages or tampers with the electronic wristband or electronic gateway device described above shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding six months or to both.	and ensuring that the personal data is not used for other purposes without consent or authorisation under the law. In particular, collection of personal data for Government's contact tracing purposes should only be done through the use of SafeEntry. The data collected will only be stored in Government's servers and used for contact tracing purposes by the Government. When implementing SafeEntry, organisations should put in place measures to ensure the safe and secure collection of personal data. For more information: www.pdpc.gov.sg/help-and-resources/2020/03/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing. **Government and public officials** The Government of Singapore is not bound by the PDPA. However: (a) there are data security provisions in the Public Sector (Governance) Act 2018 (PSGA). For example, public officers who recklessly or intentionally disclose the data without authorisation, misuse the data for a gain, or re-identify anonymised data may be found guilty of an offence and may be subject to a fine of up to $5,000 or imprisonment of up to two years, or both; and (b) there are, additionally, internal Government guidelines on the handling of data. Together with the PSGA, an independent review by the Public Sector Data Security Review Committee Report in November 2019 found that the data protection requirements imposed on the Singapore Government are 'no less stringent than the PDPA's'.

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	▪ The Government has announced that TraceTogether will cease functionality at the end of the outbreak, as indicated by an official shifting of DORSCON (Disease Outbreak Response System Condition) levels to green. When that happens, users will receive an update on how they may delete data. **TraceTogether Token** The 'TraceTogether Token' is a physical token, for voluntary adoption, that functions similarly to the TraceTogether App by using Bluetooth signals to detect other nearby TraceTogether devices. The Token is a standalone device that will be distributed to all Singaporean residents for free and is intended to benefit individuals who do not have a smart phone on which to download the app or those who do not wish to download the app on their phones. As with the app, the Tokens only record that other TraceTogether devices have been in proximity with it and this information will be encrypted and stored on the Token. If the holder of the Token tests positive for Covid-19, MOH will seek consent to access the data stored on the Token for contact tracing. Additional details: ▪ Like the App, the Token only captures proximity data via Bluetooth technology and does not capture GPS/geolocation data. ▪ The encrypted data is kept on the device until the user consents to share it with MOH for contact tracing. ▪ The token does not have internet/cellular connectivity. This means that no one can access the data remotely. ▪ To strengthen community engagement, GovTech organised a 'tear down' event to publicly confirm that the Token would only perform what it was set out it do – that is, only Bluetooth-related activities and cannot process GPS, Wi-Fi or cellular, nor record conversations. See: www.tech.gov.sg/media/technews/2020-07-06-tracetogether-token-teardown.		

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	For more information: https://support.tracetogether.gov.sg/hc/en-sg. **SafeEntry** SafeEntry is a national digital check-in system that logs the NRIC/FINs (ie, national identification numbers) and mobile numbers of individuals visiting various public venues to facilitate contact tracing and identification of Covid-19 clusters. Individuals check-in/out from SafeEntry at entry/exit points using any of the following methods: (a) scan QR code: Use the SingPass Mobile app, TraceTogether app, mobile phone's camera function or a recommended QR scanner app to scan a QR code and submit personal particulars; or (b) scan ID card: present an identification card barcode (eg, NRIC, Passion card, Pioneer Generation card, Merdeka Generation card, driver's licence, Transitlink concession card, student pass, work permit, SingPass Mobile app, TraceTogether app) to be scanned by staff; or (c) select from list of nearby locations: use the SingPass Mobile app's 'SafeEntry Check-In' function to select a location and check in. It is mandatory to provide information for all the fields (ie, ID number and mobile number). The data collected via SafeEntry is encrypted and stored in Government servers, which will only be accessed by the authorities when needed for the purpose of preventing or controlling the transmission of Covid-19. The Government is the custodian of the data submitted by individuals and there are stringent measures in place to safeguard the personal data (see response to Q3). Only authorised public officers will have access to the data. For more information: https://support.safeentry.gov.sg/hc/en-us.		
United Kingdom	In September 2020, the UK Department of Health and Social Care (DHSC) launched the NHS COVID-19 app for use in England and Wales. Download and use of the	No existing laws have been used to track citizens. Physical enforcement of restrictions and requirements of the national lockdown in England	The privacy notice of the app outlines the legal basis for processing personal data under the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA). These include characterising the processing as

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
	app is voluntary. The app does not hold any information that could directly identify an individual, such as a name, address, date of birth or unique identifier for a person's phone. The app uses the Apple-Google Exposure Notification API. The app uses Bluetooth Low Energy to record contact tracing data, including how long a person is close to another app user and the date and time of these encounters. It records the signal strength of other anonymous app users' Bluetooth to work out how far apart persons were. Contact tracing data stays on a person's phone for 14 days. The app does not assess or track a person's location. The app also uses venue check-in data, which is protected data about which venues a person checked-in to and at what time. This data never leaves a person's phone and is automatically deleted after 21 days. The app also uses the first part of a person's postcode district, to learn about the impact of Covid-19 and to predict and manage demand on local hospital services. The postcode data is not considered personal data as it is fully anonymous. If a person has a positive Covid-19 test result, consent will be sought to share that information with others who have been in contact with that person. Random unique IDs are used as part of the contact tracing technology. No personal data is shared between one person's phone and another, and the app uses complex cryptography to protect the App user's anonymity. The random unique IDs will be uploaded to a central system, the DHSC secure computing infrastructure, hosted on Amazon Web Services UK, which will then add these IDs to the list provided to every App user's phone.	are covered by a specific government regulation from 5 November 2020.	necessary for the performance of official tasks carried out in the public interest, managing a health service and public health purposes. Aspects of the app's functionality, namely access to data stored on the phone and storing data on the phone, are governed by the Privacy and Electronic Communication Regulations 2003 (as amended). The DHSC also prepared a Data Protection Impact Assessment (as required under the GDPR in these circumstances) explaining how the app complies with the GDPR, DPA and the Information Commissioner's Office's Contact Tracing Principles and app design responses. The impact assessment also addresses the Information Commissioner's specific concerns about the previous iteration of the app. The DHSC issued four notices under the Health Service Control of Patient Information Regulations 2002 which require NHS Digital, NHS England and Improvement, health organisations, local authorities, GPs and other bodies to process information. This allows patient data to be shared with organisations involved in the response to Covid-19, for example, enabling notification to members of the public most at risk and advising them to self-isolate. The DHSC has stated that it expects these organisations to share patient data within the legal requirements set out under the GDPR.
United States	The federal government has not, but some states have done so.	No.	▪ Health Insurance Portability and Accountability Act (HIPAA) – if the app is in any way connected with a health care provider, arguably it triggers the application of HIPAA. At least some of the states have established partnerships with public hospitals related to their data and, therefore, this is a potentially significant issue. ▪ Privacy disclosures – if you are a private company providing the app service for the state, but you are the one collecting the data, you likely must comply with California Consumer Privacy Act's disclosure requirements and provide rights to the individuals' whose information you are collecting. ▪ Children's privacy – there are a variety of consent-based laws that would need to be followed before children could provide information through the app.

Country	Question 1: Has the government sponsored any form of tracing app to track Covid-19 infections?	Question 2: Has the government used any existing laws to track citizens, for example, using existing telecommunications laws to track citizens who are infected to ensure they stay in quarantine?	Question 3: How do the arrangements referred to in Questions 1 and 2 interact with data protection laws or guidelines, recommendations or other relevant regulations issued by the competent data protection authorities?
			▪ Family Educational Rights and Privacy Act (FERPA) or state law equivalents – if the app is specific to a public school system or a higher education system, arguably there are FERPA implications if you are pre-populating the app with student information. ▪ Geolocation data – some states regulate the collection and use of specific geolocation data and, therefore, if the app is collecting this, it is potentially in play. ▪ Biometrics – depending on how the app works (if it is collecting temperature readings or fingerprints for login purposes, for example), there are different state laws that could be implicated. ▪ Data security – several states have mandatory cybersecurity laws for government entities. Therefore, the app would have to comply with those obligations (assuming it was the government operating the app). Otherwise, Massachusetts and New York have cybersecurity laws that would apply to private companies.