INTERNATIONAL ASSOCIATION
OF YOUNG LAWYERS

REPORT ON TECHNOLOGY MEASURES IN COVID-19 LEGISLATION

A report by the AIJA IP/TMT Commission - June 2021 (update)

Based on questionnaire amongst members, includes 21 country reports

Contributing editors:
Silvia van Schaik, IP/TMT Commission President
Árpád Geréd, IP/TMT Commission Past President

Table of contents

Introduction

In times of COVID-19 we quickly noticed that we often asked each other: how is it in your country? Being lawyers the topic quickly turned legal. To combat the spread of COVID-19, governments all around the globe have implemented measures, many of them significantly limiting freedoms which we take for granted and are also essential in a democratic society.

For example, governments implemented measures to track the movement of persons and, should they be tested positive, identify the people they have been in contact with. This tracking and identification are often achieved by technological means, such as with the help of apps or mobile phone data. Already before COVID-19 data protection and privacy and the identification of individuals - mostly by private companies - through browsers or mobile apps have been hot and controversial topics. The potential problems seem to intensify when governments employ the same techniques and measures they may have criticised and tried to reduce before.

AIJA is an international association of lawyers all over the world. The members of AIJA's IP/TMT commission deal with a broad range of topics in the fields of technology, intellectual property, telecoms, privacy and media. Especially IT and privacy lawyers have dealt with the issues described above for years. As such we are in the unique position to gather information on what type of technology-related measures governments around the globe have introduced or are planning, their acceptance and impact.

We have gathered the information by creating a questionnaire and asking our members to answer these. We received input from 21 countries, ranging from Belgium to Brazil and from the USA to Hong Kong.

In this report we:

- First, provide you with an overview of the results in a quick reference table, followed by a summary;
- Second, provide you with the names and contact details of our contributors;
- Third, provide you with the answers to the questionnaire per country.

The first edition of this report was published in November 2020 (available here). As the situation evolved, we decided to create this updated report in June 2021. We thank all contributors for their continued efforts!

Enjoy your read!

Árpád Geréd and Silvia van Schaik

Past and current President of the AIJA IP/TMT Commission

Quick reference table

	Legislation on tracking (apps)	End date	Voluntary tracking (apps)	Sharing other tracking data	Other tracking methods
Argentina	Yes, mandatory only for inbound travellers	No	Yes, governmental, same as mandatory one	No	Yes, voluntary
Austria	No	No	Yes	Yes, anonymous	Yes, mandatory registration of customers, that are expected to stay in gastronomy, accommodation facilities or non-public sports and recreational facilities for more than 15 minutes.
Belgium	Yes, database	Undefined (the day of the publication of the Royal Decree proclaiming the end of the COVID-19 epidemic).	Yes	Yes, anonymous	Yes: Passenger Locator Form for travellers from abroad; identification of foreign employees; contact data of horeca clients.
Brazil	No	No	No	Yes, required by government	No
Chile	No	No	No	No	No
Croatia	Yes, cross-border data exchange	No	Yes, governmental app	No	No
Czech Republic	No	No	Yes, governmental app	Yes, on voluntary basis	No
France	Yes, not mandatory	Yes, 31.12.2021 regarding processing of data	Yes, governmental app and others	No	No, not yet
Germany	Yes, not mandatory or specific	No	Yes	Yes, anonymous, not government	Yes, customers
Hong Kong	Yes, mandatory for inbound travellers	Yes, 30.9.2021 (subject to renewal)	Yes, governmental app (mandatory in some cases)	No	No
Hungary	No	No	Yes, governmental app	No	Yes, voluntary employer data processing regarding immunity to coronavirus
India	No	No	Yes, governmental app (mandatory in some cases)	No	Yes, regarding testing
Italy	Yes, not mandatory	Yes, 31.12.2021	Yes, governmental app and locals	Yes, anonymous	Yes, provision of contact details in some cases.
Netherlands	Yes	Yes, 10.07.2021	Yes	No	Yes, voluntary
Slovakia	Yes, for quarantine	Yes, 31.12.2020	Yes	Yes, required by government	No

Spain	Yes, through telcos	No	Yes	Yes, required by government	Yes, contact tracing apps
Sweden	No	No	No	Yes, one operator, anonymous	No
Switzerland	Yes, not mandatory	No	Yes, governmental app	Yes, one operator, anonymous	Yes, mandatory provision of contact details in some cases
Taiwan	Yes, for quarantine	No	Yes	Yes, required by government or voluntarily	Yes, contact-information registration.
UK	No	No	No, but trials existed	No	No
USA	No	No	No	No	No

Summary

The questionnaire has shown that, while the COVID-19 pandemic is global, the technological measures which affected countries use to stop the spread of the virus are different. This goes so far that of the 21 countries surveyed not even two, which employ or endorse some type of technological measures aimed at reducing infection rates, make use of the same method or system, much less have the same policy. This applies even within the EU.

An interesting result was that very few of the surveyed countries have introduced general mandatory technological tracking and identification measures in the form of software, such as mobile phone apps. Rather many of them have chosen to only oblige certain groups, such as infected individuals or travellers, or people wanting to enjoy certain activities or facilities to use (or subject themselves to) the measures while others endorse voluntary use only. At the same time most governments oblige entities possessing large amounts of tracking- and identification-data, usually mobile operators, to share that data with governmental or state authorities or agencies. Many times, the data is anonymised before transmission, in many countries however, the data is transmitted in individualised form, allowing the identification and tracking of single natural persons.

The answers to the questionnaire have further shown, that many times the measures taken by countries during the COVID-19 pandemic, be they still in effect or not, have lacked transparency and at times still do. It was therefore sometimes impossible for the reporters to ascertain that the information they provided, whether relying on official sources or not, was truly accurate. It is concerning that this phenomenon was not limited to countries known for authoritarian policies but also occurred in countries which are perceived as possessing well-functioning democratic structures. On the one hand the results indicate that many of the perceived in-transparencies have occurred at a time when the pandemic was new and unknown. Often the measures taken have been clarified or ceased in the meantime. On the other hand, there are governments that have at least planned to make use of data collected during the pandemic or to pool existing databases, originally with the aim of containing the pandemic but also with the option of other uses and thus effects that may outlast the pandemic.

As the pandemic continues to affect countries and individuals and new knowledge of the COVID-19 virus and its steadily appearing mutations is gained, countries are forced to continue with their actions to prevent the spread of the virus, fine-tuning their measures, not least to prevent further or alleviate lockdowns. While some countries are expecting to mostly return to “normality” as before the pandemic, many are continuing to prepare for a longer fight against the virus. Therefore, the technology-related measures taken today may be ceased, adapted or perhaps at times even exchanged altogether over the coming months.

Contact information of contributors

Argentina

Diego **FERNÁNDEZ**

Marval O'Farrell Mairal

Buenos Aires, Argentina

dfer@marval.com

Austria

Árpád **GERÉD**

Maybach Görg Lenneis Geréd Rechtsanwälte GmbH

Vienna, Austria

a.gered@mglp.eu

Alexandra **PRODAN**

Maybach Görg Lenneis Geréd Rechtsanwälte GmbH

Vienna, Austria

a.prodan@mglp.eu

Belgium

Louis-Dorsan **JOLLY**

ALTIUS

Brussels, Belgium

louis-dorsan.jolly@altius.com

Brazil

Luana Anastácia **MUNIZ DE BARROS**

Montaury Pimenta, Machado & Vieira de Mello

Rio de Janeiro, Brazil

luana@montaury.com.br

Chile

Antonio **VARAS**

Porzio, Ríos, García

Santiago, Chile

avaras@porzio.cl

Croatia

Željka **IVANAC**

Law Office Skerlev

Zagreb, Croatia

zeljka.ivanac@skerlev.net

Branko **SKERLEV**

Law Office Skerlev

Zagreb, Croatia

branko.skerlev@skerlev.net

Czech Republic

Štěpán **ŠTARHA** and Vojtěch **BARTOŠ**

Havel & Partners

Prague, Czech Republic

stepan.starha@havelpartners.cz

vojtech.bartos@havelpartners.cz

France

David **ROCHE**

Aramis Law Firm

Paris, France

roche@aramis-law.com

Jean-Philippe **ARROYO**

JP Karsenty & Associés

Paris, France

jpharroyo@jpkarsenty.com

Germany

Dr. Johannes **STRUCK**

Brödermann Jahn Rae GmbH

Hamburg, Germany

johannes.struck@german-law.com

Hong Kong

Felix **YUEN**

PricewaterhouseCoopers Hong Kong

Hong Kong

felix.yuen@hk.pwc.com

Hungary

Dr. András **CSENTERICS**

Réti, Várszegi & Partners Law Firm

Budapest, Hungary

andras.csenterics@pwc.com

Dr. Miklós **KLENANC**

Dr. Klenanc Miklós Law Firm

Budapest, Hungary

miklos.klenanc@gmail.com

India

Dhruv **KAKAR**

S. C. Ladi & Co.

New Delhi, India

dhruv.kakar@scladi.com

Italy

Laura **LIGUORI**, Eleonora **CURRELI**, and Livia **PETRUCCI**

Portolano Cavallo

Rome and Milan, Italy

lliguori@portolano.it

ecurreli@portolano.it

lpetrucci@portolano.it

Netherlands

Silvia **VAN SCHAIK**

bureau Brandeis

Amsterdam, the Netherlands

silvia.vanschaik@bureaubrandeis.com

Chantal **BAKERMANS**

Penrose

Amsterdam, the Netherlands

c.bakermans@penrose.law

Slovakia

Štěpán **ŠTARHA** and Adam **KLIŽAN**

Havel & Partners

Bratislava, Slovakia

stepan.starha@havelpartners.sk

adam.klizan@havelpartners.sk

Spain

Cristina **HERNANDEZ-MARTI PEREZ**

Hernandez-Marti Abogados

Barcelona, Spain

cristina@hernandez-marti.com

Sweden

Anna **EIDVALL** and Maria **JENNERHOLM**

MAQS Advokatbyrå AB

Gothenburg, Sweden

anna.eidvall@maqs.com

maria.jennerholm@maqs.com

Switzerland

Janine **REUDT-DEMONT**

Niederer Kraft Frey AG

Zurich, Switzerland

janine.reudt-demont@nkf.ch

Kaj **SEIDL-NUSSBAUMER**

Probst Partner AG

Winterthur, Switzerland

kaj.seidl-nussbaumer@probstpartner.ch

Taiwan

Sophia **YEH**

Tsar & Tsai Law Firm

Taipeh, Taiwan

sophiayeh@tsartsai.com.tw

United Kingdom

Chloe **TAYLOR**

Carpmaels & Ransford

London, UK

chloe.taylor@carpmaels.com

Zoe **WALKINSHAW**

Bristows

London, UK

zoe.walkinshaw@bristows.com

United States of America

Katja **GARVEY**

Kegler Brown Hill + Ritter

Columbus, Ohio

kgarvey@keglerbrown.com

Report per country

Argentina

Contributor(s): Diego Fernández, Marval O'Farrell Mairal, Buenos Aires, dfer@marval.com.

Last updated: 28 May 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	At a national level, the Argentine Government has implemented a mobile app named "COVID-19 Ministry of Health", which has geolocation functions. *Status of the legislation* Administrative Decision No. 432/2020 (in force since 24 March 2020) established the mandatory use of app "COVID-19 Ministry of Health" for those who had entered the country in the last fourteen days, and for those who do so in the future. In addition, Provision No. 3/2020 (in force since May 6, 2020) created a database to process the data generated through the aforementioned app, while Provision No. 4/2020 (in force since May 21, 2020) approved and made public its terms and conditions. On October 14, 2021, the Argentine Undersecretariat of Open Government, which depends on the Secretariat of Public Innovation of the President's Chief of Staff Office, approved a new version of the Database of the App "COVID-19 Ministry of Health" in order to centralize the data collected by the application. This expansion allowed a larger flow of information to be processed and improved usability by citizens. *New or existing data* App "COVID-19 Ministry of Health" gathers new personal data, which is provided directly by its users, except for those related to voluntary geolocation (obtained automatically from the data subjects mobile devices). *Access* The Argentine Undersecretariat of Open Government is responsible and has access to data provided by app "COVID-19 Ministry of Health". Moreover, the

		Undersecretariat may transfer such personal data (whenever possible, in a dissociated form) to other state entities and/or national, provincial or municipal health facilities. *Safeguards* Provision No. 3/2020 provides that the data collection carried out through "COVID-19 Ministry of Health" should comply with provisions of Argentine Data Protection Law No. 25,326, in particular, the principles of lawfulness, data quality, purpose limitation, informed consent, confidentiality and security. *End-date* This measure has no end-date and is expected to last as long as the health emergency declared by the Argentine Government remains in force.

2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	As mentioned at Question 1, the Argentine Government has implemented "COVID-19 Ministry of Health" app. Notwithstanding its mandatory use by inbound travelers, it is voluntary and the Government recommends its use to anyone who resides in Argentina. This app provides guidance and/or instructions on how to get to the nearest health facility, as well as preventive or health assessment assistance measures. Moreover, this app uses geolocation functions to make comparisons and predictions, such as mapping of risk areas, and – according to statements – it does not identify people who the user was in contact with. Similar apps have been deployed at a provincial and municipal level. *Developer and provider* The Argentine Ministry of Health and the Argentine Secretariat of Public Innovation of the President's Chief of Staff Office are the developers and providers of app "COVID-19 Ministry of Health". *New or existing data* App "COVID-19 Ministry of Health" gathers new personal data from its users. *Access* The Argentine Undersecretariat of Open Government has access to data provided by app "COVID-19 Ministry of Health", in addition to any other state entities and/or national, provincial or municipal health facilities to which the data may be transfered. *Use and acceptance of voluntary measures* App "COVID-19 Ministry of Health" is a self-evaluation mobile app that allows its users to answer some questions related to their health status and symptoms.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	To the best of our knowledge, no.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	At a provincial level, Santa Fe, La Rioja, Tierra del Fuego, Misiones, Río Negro, Buenos Aires, Mendoza and Jujuy have official apps (similar to "COVID-19 Ministry of Health" national app). At a municipal level, La Matanza (Buenos Aires) has recently developed a software called "CovidControl", which operates through a mobile app, and allows the local government to assist COVID-19 patients as well as those suspected cases, who have 24-hour medical monitoring but are also subject to follow up on their compliance with the mandatory isolation. Moreover, the Agency of Access to Public Information (controlling authority of the Data Protection Law No. 25,326) has recently published a series of recommendations for the use of geolocation apps, listing fundamental principles on data protection applicable to them (whether they are used by the public or private sector, or both in collaboration). Among others, the Agency recommends a privacy impact assessment to be carried out prior to the implementation of this type of apps in order to control and mitigate its risks, as well as to assess its feasibility. Moreover, the Agency has recently issued guidelines regarding temperature checks by public and private entities that help data controllers to comply with data protection regulations. Through Provision No. 06/2021, the Undersecretariat of Open Government created the COVID-19 Vaccination database in order to organize, streamline and the carry out the administration of vaccines authorized by the entities and jurisdictions with competence in the matter against COVID-19, and thus contribute to the prevention and limit the health consequences of the virus. The registry contains the doses of COVID

		vaccines applied and reported by the 24 provinces, and the most relevant data of the vaccination process throughout the country: department or municipality, age groups, sex, place of residence, place of application, date, type of vaccine and dose applied, among others. The reported cases are anonymized. The Undersecretariat will transfer the personal data of the users only in the context of the health emergency declared by the Administrative Decision No. 260/2020 and within the framework of the faculties of the transferee entities. Whenever possible, the Undersecretariat will transfer such personal data in a dissociated way. Furthermore, the Agency for Access to Public Information published the Guide for Access to Information, Personal Data and Vaccination against COVID-19, which describes a series of criteria for the treatment and disclosure of personal data of people who are vaccinated against COVID-19. The Guide seeks to achieve a balance between the citizens' right of access to public information and the right to privacy of the data subjects.

Austria

Contributor(s): Árpád Geréd and Alexandra Prodan, Maybach Görg Lenneis Geréd Rechtsanwälte GmbH, Vienna,a.gered@mglp.eu, a.prodan@mglp.eu.

Last updated: 10 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Austria has not yet introduced any legislation on the electronic tracking of individuals, though the mandatory use of the (as yet voluntary) app “Stopp Corona” is discussed. Austrian mobile operators have been obliged to provide statistical data, such as data on the mobility of customers, with the aim to better combat the spread of COVID-19. However, such data is anonymous and neither intended nor used for contact-tracking.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	For general COVID-prevention, the Austrian Red Cross has developed the mobile app “Stopp Corona”. This app is also the one promoted by the Austrian government. While the government did not participate in the development, the Red Cross did cooperate with UNIQA (an insurance agency, for financing) and Accenture (for development aid, maintenance and backend provision). Accenture uses Microsoft Azure to host the app and data. The app is available for Android an iOS phones and uses the Exposure Notification Frameworks provided by Google and Apple respectively. An enabled Bluetooth connection is required for the use of the app. The app displays a warning notification, should Bluetooth be turned off. Upon installation and periodically afterwards, 2 random IDs and a code are generated by the Exposure Notification APIs: - Temporary Exposure Key (TEK): Once per day - Rolling Proximity Identifier (RPI): Once about every 10 minutes, generated based on the TEK

		- Security Code: Once every 14 days When devices with activated “Stopp Corona” apps are within 2m of each other for more than 15 minutes, the apps exchange the RPIs (“digital handshake”), which are then stored on the devices. Due to the high frequency of the changes to the RPI, tracing of the movements of a single person should be impossible. The possibility to manually initiate a handshake has been implemented originally but removed in June 2020 due to changes in the Exposure Notification Frameworks. In case an infection is reported, the users are notified if they have been in contact with the respective RPI during the last 2 days. The 2-days restriction is not based on data protection concerns, but rather on infection statistics. To make an infection notification, a user always has to provide their mobile number. A TAN is sent to the reported number, which then needs to be entered for the notification to be sent. Furthermore, the TEK is transmitted and the security code is used to technically authenticate the notification to the central server. Once per day, each app connects to the server and retrieves the lists of all TEKs from the last 2 days. Then it calculates the RPIs and compares those to the RPIs stored on the device. In case of a match, the user is alerted. As far as data protection and security is concerned, the “Stopp Corona” app has been reviewed and approved by data protection NPOs epicenter.works and NYOB, as well as research institute SBA-research. Furthermore, the source code is available for review. Lacking any as yet discovered relevant faults, it is therefore considered safe and compliant. Nevertheless, the app has seen relatively little acceptance yet. According to the Red Cross, as of 5 October 2020 the app has been downloaded about 1.038.431 times on both Android and iOS devices. While equalling roughly 12% of Austria’s

		population, this number includes potential re-downloads. Since June 2020, 335 confirmed and 1476 potential infections were reported through the app. As of 19th May 2021 registration of customers, that are expected to stay in gastronomy, accommodation facilities or non-public sports and recreational facilities for more than 15 minutes, is mandatory. This also applies to visitors of events and fairs. The relevant regulations did not specify any method but merely required that the restaurant obtains the following data from the customer and stores it for a period of 4 weeks: - name - surname - telephone number - e-mail-address (optional) - date of visit - time of arrival - table number. On the one hand, there are template registration sheets for gastronomy-operators and accommodation providers, on the other hand operators of gastronomy and hotels are free to use electronic methods, which are usually provided as paid services (however, some are free) by various national and international companies. Customers usually register themselves by scanning a QR-code provided by the operator with which they are redirected to a webpage already displaying the name of the operator they are in and then providing the first 3 (or 4) pieces of data mentioned above. Customers can then also decide whether their contact data should remain saved in the app for future use or not. Speaking of non-public sports and recreational facilities as well as events and fairs, “registration” is usually effected by customers/visitors registering in advance with the data mentioned above or disclosing this data to the operator prior to entry. The customer-data is encrypted on the device and then transferred to the

		servers, where it is saved for 28 days and then deleted. Health authorities can request the registered data. However, operators may process and transmit the data exclusively for the purpose of contact tracing and must take appropriate data security measures in connection with the processing and transmission of such data and in particular, ensure that the data is not available to third parties. All requests by authorities are documented, though it is unclear to which degree of detail. The systems have already been criticised for being centralized as well as being closed-source. Both in contrast to the “Stopp-Corona-App” of the Red Cross, which is viewed as the system that better safeguards privacy.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	In mid-March it has been discovered that at least telecommunications and mobile operator A1 (formerly “Telekom Austria”, the state-held monopolist) provided customer data to the federal government as of probably the beginning of the pandemic in Austria in early March. While the newspaper claimed that the transmitted data also contained information on individuals, A1 has admitted to having transmitted customer data to the government but that the tracking of individuals based on the data provided was “inconceivable”. It is still unclear, which concrete data was provided to which government or state agencies. Also the legal grounds are not known. The government has merely stated that it was entitled to demand certain data from telecom providers in “cases of emergency”. Furthermore, it is unclear, whether the other mobile operators have provided any data to the government in the context of COVID-19-prevention. As the discovery was made almost exactly at the time of the lockdown in mid-March 2020 and since the provision of data by the mobile operators has been transparently regulated by the end of the same month, the open questions will remain so for the foreseeable future.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	The Medical University of Innsbruck, in collaboration with the Provincial Institute for Integrated Care Tyrol (“Landesinstitut für Integrierte Versorgung”) and the Austrian Institute of Technology, has developed a possibility of tele-medical monitoring for quarantined patients. A similar project that has already existed in Tyrol since 2017 for patients with heart failure served as a model. The aim is for patients in domestic quarantine to be able to stay at home as long as possible, but to be taken to hospital in good time if their condition deteriorates, whereas “in good time” means, that they are taken to hospital, when a treatment in the intensive care unit is not yet necessary in order to conserve capacity.

		This kind of monitoring is voluntary and only affects patients who tested positive and registered for it by phone or e-mail with the medical university. Registered patients then receive devices - namely ear-/skin sensors as well as an application. The sensors automatically measure the patients' health values, such as body temperature, oxygen saturation, respiratory rate, etc. and transmit them to a team of about 20 people at the medical university, that is available 24/7 and is notified in case of deterioration. This monitoring runs for an initial period of 3 weeks, but can be extended or shortened if necessary. Also, the city of Vienna has set up a WebApp called "Homecare" for people in domestic quarantine, who will automatically get the link to the App. On the one hand, this WebApp contains useful information. On the other hand, people can use it to electronically submit their health status to the health authorities using an online form. In this context, the City of Vienna requests the daily transmission of information on the current state of health. In addition, the health status of those persons who are in domestic quarantine together with the person concerned should also be communicated. However, it is clarified that the "Homecare"-WebApp does not have any legal effect and therefore does not constitute a notice. A similar project does also exist in Tyrol, where people, living or staying in Tyrol, can register themselves online as "suspected case" or "contact person". In addition, the so-called "green pass" shall be introduced on a national basis as of June 10th or 11th 2021. This will be a simple, secure and verifiable proof (certificate) of vaccination, a recent (max. 6 months ago) infection with SARS-CoV-2 or a negative test. Each of these certificates shall be provided with an individual QR code,

		which will form the basis for verification and will therefore constitute an “admission ticket” for e.g. gastronomy, cinemas or gyms (PDF documents with individual QR code). These certificates can be easily saved and presented on electronic devices or printed out and presented in analog form. However, a mobile signature or citizen card is required to retrieve the certificates digitally. The “green pass” certificates are a supplement to the now existing proofs (such as officially recognized vaccination certificates, segregation notices or test certificates), which will still be valid. Therefore, there will be no obligation to use the "green pass". However, scanning a QR code surely is easier and faster than checking a filled document. However, it remains to be seen, whether the Austrian "green pass" will actually be launched as early as June 10th or 11th, as there currently seem to be problems with the technical implementation of the digital version. In any case, it is clear that vaccinated persons will still have to be patient for a while and that the Austrian “green pass” will for now only be implemented for persons tested negative and recovered in the 1st stage. The implementation for vaccinated persons is not yet possible due to technical challenges, but is expected to take place by the beginning of July, when, according to current information, the "green pass" shall also be introduced at European level. From this date at the latest, it will certainly become considerably more important - especially for travelling abroad. Last, but not least, it should also be mentioned, that the initial draft of the amendment to the Austrian Epidemic and Covid-Measures-Act, with which the “green pass” mentioned above should be implemented, originally also envisaged a large-scale collection of data from almost all citizens ("super database"). Specifically, a registry was to be created

		that would combine data from Covid-19 sufferers and vaccinated individuals and link it to their data on work life, income, periods of unemployment, education, rehab stays, and sick leaves. In addition, it was also envisaged, that the Federal Minister of Health should be authorized to request additional data from all other ministries by decree. This project was (self-evident) heavily criticized and shall no longer be implemented. Nevertheless, this example shows how easily measures to combat pandemics can be used for excessive purposes - even in countries like Austria, which ranks 18th according to the World Democracy Index (https://en.wikipedia.org/wiki/Democracy_Index).

Belgium

Contributor(s): Louis-Dorsan Jolly, ALTIUS, Brussels, louis-dorsan.jolly@altius.com.

Last updated: 07 June 2021

	Question	**Answer**
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Since the outbreak of the pandemic in March 2020, the Belgian institute of public health *Sciensano* has been systematically collecting data on COVID-19 contaminations, hospitalisations and deaths in a COVID -19 database. The legal basis of this COVID -19 database has only been created *a posteriori* through temporary Royal Decrees (nr. 18 and nr. 44) and eventually through the Cooperation Agreement of 25 August 2020 between the Belgian federal government and the federated entities (endorsed by the federal Act of 9 October 2020 and which applies retroactively), which have also set out the legal framework for *manual* and *digital* contact tracing. In short, the contact tracing in Belgium relies on 3 core elements: **1.** A central **COVID -19 database** fed by the doctors, hospitals and laboratories, thecontact centres and the federal e-health and social security databases. The processing of personal data in the database has the following purposes: - to identify and contact the potentially contaminated persons via the contact centre; - to carry out scientific and statistical research; - to communicate data to the regional health inspection services. **2.** **Contact centres** tasked with manual contact tracing. The staff members speak to people who have been contaminated, figure out who they have been in contact with, and then notify anyone they think may have contracted it. **3.** The **Coronalert exposure notification app** released in September 2020, which is a decentralised proximity tracing app based on the Bluetooth technology.

		Please note that the Belgian data protection authority has spoken out critically against the legal framework for contact tracing (which is based on *governmental* vs. *legislative* rules) through 7 opinions. Besides the contact tracing framework described above, the ministerial decree of 28 October 2020 sets out detailed emergency measures applicable in Belgium to limit the spread of the COVID-19 (e.g. regarding mandatory teleworking, opening of shops and restaurants, restrictions of gatherings and travels, etc.). The rules of this ministerial decree are applicable until 30 June 2021. Please note that this ministerial decree also contains some tracing-related obligations: • Employers are required to keep during 14 days a record with the identification data of all foreign workers (i.e. living or residing abroad) which they employ in Belgium for more than 48 hours. • Horeca operators are required to keep during 14 days a record with the contact data (at least one, e.g. email or phone) of one person per table. • Transporters are required to check, prior to onboarding, that any person travelling to Belgium from abroad has filled in the Passenger Locator Form (which is stored in the central COVID-19 database). The European COVID-19 certificate will be in use in Belgium as of 1 July 2021.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Yes, the voluntary use of the Coronalert tracing app has been promoted since end of September 2020.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	The 3 main telecom operators in Belgium have voluntarily joined the “Data Against Corona” taskforce created in March under supervision of the previous Belgian federal ministers of health (Maggie De Block) and digital (Philippe De Backer). This taskforce has anonymised and computed telecom data from millions of Belgians, allowing to support political decision about the confinement measures. The government did not receive any mobile phone number, name, or individual location data in this context, but only anonymised metrics that capture mobility, aggregated by ZIP code.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	N/A.

Brazil

Contributor(s): Luana Anastácia Muniz de Barros, Montaury Pimenta, Machado & Vieira de Mello, Rio de Janeiro, luana@montaury.com.br.

Last updated: 07 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	No. In Brazil there are no specific laws aimed at tracking or identifying individuals that might have been in contact with other individuals infected with the COVID-19 virus. Brazil has still not implemented its Data Protection Law ("LGPD").
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	No. While the Brazilian Federal Government only recommended measures such as the mandatory use of face masks, some Brazilian states considered the possibility of using technological measures to track individuals and identifying people that could have been infected. However, due to issues arising from the collection of personal data from such users and the possible misuse of such data by authorities, with no regulatory safeguards, governments refrained from using technological measures such as "contact tracing" apps.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	Yes. Authorities from a few Brazilian states, such as São Paulo, Pernambuco and Rio de Janeiro, have requested to mobile phone providers information on movement and/or communication data. However, such data is being used by these governments to identify specific areas and regions in which social distancing recommendation were not being followed. As an example, in the city of Recife, in the Brazilian Northwest region, has partnered with the local start up InLoco to use geolocation technology from mobile phones, without collecting any personal information, to monitor social distancing by neighbourhoods and to check percentages of people who remained at home in individual areas, as well as mobility patterns. In this specific example, the information is not requested to the mobile

		phone service providers. For additional information, please check here.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	No. Due to the fact that Brazil`s Data Protection Law is still not in force, most of the initiatives to use contact tracing apps are stalled or postponed. These initiatives have been challenged by NGOs and other groups that discuss privacy matters, due to the risk that contract tracing apps could also be collecting personal data, and personal health information (also understood as “sensitive data” by Brazilian laws) irregularly.

Chile

Contributor(s): Antonio Varas, Porzio, Ríos, García, Santiago, avaras@porzio.cl.

Last updated: 07 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	No. The only tracking system applied by Chilean authorities is through the delivering of the address information of the positive tested individuals. They are controlled by phone calls or periodic visits to their domiciles, when they are not in health institutions. In addition, individuals are randomly controlled by Police through identity controls, where the authority crosses the information of the controlled people with a governmental data base of the infected individuals. Therefore, there is no tracking in real time through applications or any other tech media.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	No. the only promoted technological mean is the use of interactive maps in order to be aware of the number of infected individuals in a certain area. Such information corresponds to the one given by the positive tested individuals mandated to be in quarantine in their domiciles.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No. There isn't public information related to these facts.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	No.

Croatia

Contributor(s): Željka Ivanac and Branko Skerlev, Law Office Skerlev, Zagreb,

zeljka.ivanac@skerlev.net, branko.skerlev@skerlev.net.

Last updated: 14 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Croatian Stop COVID-19 application was introduced on 27.07.2020. within the existing Croatian legislation. The application is in line with European Commission "Guidance on Apps supporting the fight against COVID- 19 pandemic in relation to data protection" and the European Data Protection Board "Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak" and compliant with the obligations set forth in GDPR and ePrivacy Directive. On the basis of the old Act on protection of the population from infectious diseases the Minister of Health adopted a security measure- the Decision on establishment of cross-border interoperability of a mobile application for informing users on exposure of COVID-19 for the purpose of public health interest of monitoring and control of infectious diseases which entered into force on 30.10.2020. The cross-border data exchange of the Croatian Stop COVID-19 application was the result of decisions and recommendations of the European Commission and the technical and safety requirements of the eHealth Network and other European bodies. Cross-border data exchange between national mobile contact tracking applications is defined by Commission Implementing Decision (EU) 2020/1023 of 15 July 2020. The new Act on protection of the population from infectious diseases entered into force on 5.12.2020. and enlisted the mentioned Decision in the Article 47 as a security measure decision.

2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Croatian government has introduced the Stop COVID-19 application based on the Google / Apple system "Exposure Notification". The application requires the explicit consent of the user which can be withdrawn at any time. The application is completely voluntary in all steps of use and the user fully manages the data he wants to share. COVID-19 positive users not identified by Apple and Google. Other than enabling the setting for cross-border data exchange, a person can receive notification of exposure in case of travel abroad or interaction with users of other authorized COVID-19 mobile applications in Croatia The application operates by assigning randomized keys to all mobile phones. The keys are a random string of characters and do not contain information about the device or about the personal information about the user. Keys alternate several times each hour to keep the privacy protected at all times. In the presence of another user of the application, mobile phones exchange their random keys via the Bluetooth feature. The application can track the contacts made without identifying the user or the person user was in contact with. Users who receive a positive lab result can share their random keys broadcasted in the previous period, making them available to other users of the application. Sharing random keys is done by entering the code generated for the user by a healthcare professional after receiving a positive laboratory result. The app periodically checks the keys shared with the server and compares them to the keys stored on the user´s mobile. In this way, the application can determine whether the user has been exposed to the dangers of infection. The user receives a notification if the application has found a shared key on the mobile phone and instructions on how to proceed. The application operates without the need for information about where or with whom the user has been with.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	To the best of our knowledge, no such offer has been made to the government. There is no legal ground within Croatian legislation that would allow for sharing movement and/or communication data by companies storing such data with the government or other authorities for purposes other than criminal investigation and prosecution or protection of national security and national defence.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	Except for the Decision on establishment of cross-border interoperability of a mobile application for informing users on exposure of COVID-19 for the purpose of public health interest of monitoring and control of infectious diseases by the Minister of Health and the new Act on protection of the population from infectious diseases, no legal developments regarding tracking individuals in relation tocombatting COVID-19 took place in Croatia.

Czech Republic

Contributor(s): Štěpán Štarha and Vojtěch Bartoš, Havel & Partners, Prague, stepan.starha@havelpartners.cz and vojtech.bartos@havelpartners.cz.

Last updated: 07 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	The Czech Republic has not introduced any specific or new legislation aimed at tracking individuals or identifying people they have been in contact with either by use of an app, by obtaining data from mobile operators or otherwise. Nor does it seem that the legislator is planning to do so. However, on 19 March the Minister of Health of the Czech Republic issued to that end an Extraordinary Measure which is an act of the executive branch with normative legal effects ("Measure"). - The competence of the Minister of Health ("Minister") to issue executive measures is enshrined in Section 80 para 1 letter g) combined with Section 69 para. 1 letters a) – i) of the Act No. 258/2000 Coll., on the protection of public health ("Act"). The Measure was issued under the residual competence under letter i) of the said provision to "forbid or order certain other activities for combating an epidemic or the threat of its emergence". Whether the Measure may have been issued under the residual competence or under the Act at all is disputed. Nor the Act neither any other legislation confers the competence to the Ministry of Health or Public Health Authorities ("Authorities") to process personal data specifically required by the Measure. From a constitutional and human rights perspective it is disputed whether such interference with the right to privacy may have been based on an act of executive branch and moreover of a single minister instead of an act of the entire Government as a body or better of an act of the Parliament.

		- The Measure orders (i) to mobile network operators to hand over to the Authorities traffic and location data of end users and (ii) to banks to hand over to the Authorities the data related to the use of means of electronic payments (i.e. credit and debit cards, e-wallets, etc.). Under point (ii) only data of persons who were located in an area defined by the Authorities on the basis of data gathered under point (i) shall be handed over. The data may be handed over to the Authorities only where demanded so by the individual and with their consent. In this regard the Measure is unclear or rather silent as to how and by whom and at what stage the consent is to be obtained. Moreover the Measure is rather confusing and unclear with regard to the requirement of consent as such. The wording of the Measure aims primarily on the consent with processing of data under point (i) but on the other hand it expressly states that any data may be processed only with the person's consent. - The Measure counts with processing of data which is already being processed by the respective controllers (although originally for different purposes), i.e. processing of any new data is not foreseen. - According to the Measure the data is to be accessed by the Authorities only. However in practice the Authorities cooperate on the execution of the Measure with the Army of the Czech Republic whose members operate the call centres which eventually execute the epidemiological tracing as such. - As a safeguard the Measure provides only that no collected data may be retained by the Authorities for longer than 6 hours and must be deleted right after if it is no longer necessary for the stated purpose. The epidemiological tracing is the exclusive purpose of processing. However, neither the

		Measure nor any other document with any legally binding force defines “epidemiological tracing” and activities related to it. - The Measure does not have any end date and may be repealed only by the Minister at any time (or by a court if found illegal or unconstitutional). During the autumn “second wave” of COVID-19 in the Czech Republic the Authorities use for contact tracing only mobile phone data which are obtained with an explicit consent of the infected person during a tracing call performed by an operator engaged by the Authorities. Beyond the said Measure the Ministry of Health also operates a mobile app called “e-rouška” (e-mask – nation-wide home manufacturing of masks being the symbol of the fight against coronavirus in the Czech Republic). The app was developed entirely as a private non-profit enterprise by several individuals and companies active in IT and app development and was given for free to the Ministry of Health which operates it now. However, the operation of the app is not expressly covered by the Measure or any other act of the executive or legislation. It is being operated in a legal vacuum, *preater legem* so to say. - The use of the app is entirely voluntary (although the use is very much encouraged by the Authorities). - The app is a contact tracing app which does not gather geolocation information but only anonymous data that another user of the app later indicated as COVID-19 positive was in the proximity. - The developers of the app tried to be as transparent as possible towards both the IT community and general public – information web page was created and source code of the app was published. The app’s integrity and security was audited by academic institutions and it seems to comply with the requirements of the

		European Data Protection Board's Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. During the autumn "second wave" of coronavirus in the Czech Republic the app underwent a development and is now based on the Google and Apple Exposure Notification System which allows the users to be informed in case they have been exposed to COVID-19 but does not share any personal data with the Authorities or other government agencies or users of the app. The app allows the user to indicate in the app if he or she was diagnosed with COVID-19. In such case the app sends an anonymous notification to all other users which were in contact with that person. If the user is notified by the app of the exposure it is entirely up to that person what further steps he or she will take. None of the app-produced data stored on the servers operated by the Authorities allow the identification of any particular person by the Authorities.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	The Czech Government has repeatedly and strongly recommended the use of the abovementioned app e-rouška which was originally a private enterprise. However, nowadays the app is fully operated by the Ministry of Health although no legal framework for such operation exists. Although it has not been specifically addressed by the Minister in public, it seems that the Authorities consider the app and its operation to fall under the Measure. The Authorities claim that any data within the framework of the so called "smart quarantine" (which includes both measures described under the Answer No. 1) are processed by the Authorities maximally for 6 hours and deleted afterwards. At the beginning of September, the Authorities started a national promotional campaign for the app on TV, internet and other mass media strongly encouraging its use.
3	Have any companies in your jurisdiction storing movement and/or communication	To the best knowledge of the authors no private company has offered the relevant

	data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	data to the government. However, the company Seznam.cz provider of the most popular maps services in the Czech Republic – mapy.cz, offered to the users of the maps the possibility to share their location and health status with the provider who would himself notify other persons using the app that they may have been exposed to the infection. The data is accessible to the provider only who does not share it with any third persons. The data sharing feature of the app has so far no end-date.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	The Measure was one of many issued by the Minister by which the Authorities have rather severely interfered with fundamental rights and freedoms of the individuals in the Czech Republic. Given the very debatable legal basis of the measures and procedure how they were adopted there are already cases pending at the administrative courts who will review the validity of these measures. It is probably only a question of “when” rather than ”if” that the Measure be also challenged in a court.

France

Contributor(s): David Roche, Aramis Law Firm, Paris, roche@aramis-law.com and Jean-Philippe Arroyo, JP Karsenty & Associés, Paris, jpharroyo@jpkarsenty.com.

Last updated: 17 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	The French government developed a contact tracking application named "*StopCovid*" available on the iOS and Android marketplaces since 2 June 2020. Its development has relied on technical and research assistance from companies (e.g. Orange, Dassault Systèmes, Capgemini), start-ups, foundations (e.g. Pasteur Institute) and public entities (e.g. Public Health, Army). In February, 2021, StopCovid has been replaced with a new application called TousAntiCovid which has the same role but contains new features. *Status of the legislation* The decree of 29 May 2020 implementing the StopCovid app and the processing of its data has come into force. The decree was enacted following a consultative parliamentary debate, and an advisory decision issued by the French Data Protection Authority (CNIL); political opinion remains divided. The decree has been modified by another decree dated February, 12, 2021, so as to reflect changes created by the creation of the new app TousAntiCovid. *Description* How does TousAntiCovid work? First, the appmust be installed on smartphones. The smartphones of individuals register the references of the nearby devices if two cumulative criteria are fulfilled. Those people must be in contact: - for a certain time (5 minutes), - at a certain distance (less than 2 meters). If an individual appears to be positive for COVID-19, the referenced phones are notified. Then, the users can take precautions to limit the transmission network. The app

		also presents information on the virus, symptoms and the recommended behavior to adopt. As of now, the application does not take into account particular contexts in which users could be in contact with a positive individual but not subject to contamination (e.g. health care professionals, people separated by a glass panel) → in this case, the government suggests to disactivate the app temporarily. *QR Location Codes (TousAntiCovid Signal)* Since June 9th, in places visited for an extended period of time (more than 15 minutes) and when wearing a mask is not possible at all times or when an accidental break in the barrier measures is possible (e.g., pubs, restaurants, gyms…), visitors have to flash a QR code in the app before entering such place. Depending on the type of establishment, the QR code will work for a set time (from 30mn for fast food places, up to 120mn for restaurants). By scanning this QR Code, the visitor adds locally on his phone the crypto-identifier of the establishment. He will be alerted if it turns out that, during that same time slot, another visitor who was present and contagious was subsequently diagnosed positive to Covid-19 and declared himself in the application ("orange" notification in case of possible contamination, "red" alert in case of cluster). Places that the user visited are stored for 15 days. The user has the possibility to manually delete a place. *Digital Booklet* TousAntiCovid also contains a digital "booklet" that allows users to store test certificates (PCR and antigenic) and vaccination certificates. These certificates will be necessary in order to participate in certain events. These certificates (in the form of a QR code) can be checked with a dedicated app (TousAntiCovid Verif), which is currently being tested for the verification of negative

		RT-PCR tests from France on selected air and sea routes. *Technology used* TousAntiCovid works with Bluetooth and doesnot use geo-location. On this basis, it is not supposed to track the individuals' movements. *Safeguards* According to Government's communication, several safeguards are implemented in order to ensure security, respect of individual rights and freedoms and the respect of data protection (GDPR compliant): <u>Non-mandatory application</u> - Installation of the app on a voluntary basis (13 million French people do not have smartphones); - Free app; - The use of the application must not condition access to certain services (care, tests, public transport, etc.); - Usage of location QR Codes can be avoided by filling information in a "recall booklet" and the electronic booklet can be replaced with paper certificates. <u>Consent and security</u> - Consent will be ensured at several levels: when installing the application, activating Bluetooth, notifying the positive result in the application. - Use of the 'captcha' service when installing the app to verify that it is used by a human being. - Information notices are displayed next to the Location QR-codes. <u>Anonymity and freedoms</u> - Anonymity will be respected either by the government and by the users: informed users will not be able to know the name of the person who contracted the virus, when and in which context this contact took place. - Only pseudo-identifiers are exchanged between cell phones (a series of numbers, letters or symbols) automatically renewed every 15 minutes.

		- The application will not create a namely list of infected persons but a contact list using “random and temporary pseudonyms”: no requirement to provide civil status or phone number. - No one will be able to falsely declare themselves infected: Users with a positive test will have to enter a code sent by their laboratory to declare themselves positive on the application. - It will not be possible to track infected people’s movements, contact the alerted person or monitor the respect of the containment measures or any other health recommendation. - Contact with health care personnel if there is a risk of infection will only be recommended - not mandatory. - - The app encourages people under 15 to discuss whether to install the app with their parents or their legal guardians. - The history of visits, stored on the user's phone, is made up of identifiers of the establishments visited which makes it difficult to find the name or address of said establishments. <u>Transparency</u> - Open-source code and free access. - The cryptographic algorithm meets the security baseline and uses the SKINNY-CIPHER64/192 encryption algorithm as recommended by the general security reference of the French National Agency for the Security of Information Systems (ANSSI). - Bug bounty in process: the source code is released to let hackers test its security and identify loopholes. *Storage and deletion of data* - Data stored on the phone and on the server for 14 days, and automatically erased after this period. - The proximity history data of contacts at risk of contamination are stored on the server for 15 days after their collection.

		- A user can delete data stored on the phone, data stored on the server as well as data relating to their registration. *Recommendations of additional safeguards* The initial recommendations of the French data protection authority (CNIL) (better information, specific information for minors, right to erase data) have been implemented with the change from StopCovid to TousAntiCovid. With regards to new developments, the CNIL has recommended the source code of TousAntiCovid to be published. Regarding the “recall booklet” (replacing Location QR codes) : - The data collected must be limited to the client's identity (name/first name), telephone number, and the date and time of arrival: it is forbidden to collect more information; - Only the appropriate health authorities may request the recall booklet; - Clients must be clearly informed of the purpose of the recall booklet and of their rights regarding their data; - The booklet should not be left in view of all the customers: it is recommended to provide an individual form or one per table. *Access* Data will be processed in a mixed system: centralised and decentralised. Indeed, if no central server was used, then the list of patient identifiers would have to be stored locally on each user's smartphones. Then, data will be partially centralised on a general server storing pseudonymous identifiers of persons exposed to the disease. This server is managed by health authorities. The list of QR Codes, corresponding to places that have been frequented by people who have tested positive for Covid 19 are stored on a dedicated, highly secure central server, which is separate from the server on which other data is

		stored. The comparison between the list of places visited by the user and the list of places visited by Covid+ people is made directly on the user's phone. In order to do this, the app regularly downloads the list of places at risk (which is stored in the central server). Test and vaccination certificates are only stored in the user's cellphone. The system is different from the solution developed by Apple and Google. Personal data will not be transferred outside the EU. The French Minister for Health is the data controller of this data processing: if the application evolves, it will have a link with the competent national health authority. Plus, the provider of the infrastructure hosting the application acts as a processor and is certified as a Health Data Hosting and Cloud Computing Service Provider by the authorities. The Government indicates that the encryption keys for IDs will be protected and will be entrusted to entities of different nature (private, public, independent, etc.) to prevent a single actor from possessing all of them and hijacking data. *End-date* The principle of proportionality requires that the rights to privacy and personal data should not be infringed for a longer period of time than necessary. Several measures are announced on this basis: - The processing of the data will stop after December 31st, 2021; - The proximity history data is stored for fifteen days after it was recorded (on both the server and the cellphone); - Location QR codes are stored for no longer than 24 hours. A report on the operation of the application will be published before January, 30th, 2021.

2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	The government did not recommend the use of another app.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No, but alternative solutions have been developed by Google and Apple, and have been presented to the French government, which has preferred developing its own solution.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	Doubts remain regarding the actual transparency and centralised processing of data. The National Consultative Commission on Human Rights, the Paris Bar Association and several civil liberties NGOs have expressed concerns and have pointed out a manifestly disproportionate infringement of the rights and freedoms of citizens by such an application. Following a law voted by the Parliament, which has substantially amended the bill presented by the government, a centralised information system has been created and implemented to identify individuals bearing COVID-19. Safeguards have been provided by the Parliament in order to limit the infringement of civil liberties, including privacy. This system is not based on applications or IT tools, but on a network of medical staff and entities in order to monitor and limit the spread of the virus. The French Data Protection Authority (CNIL) has also issued an advisory decision in relation to this information system. There should be more development in the coming months, especially regarding the measures implemented by the government due to the end of the state of sanitary crisis. The CNIL has already highlighted in a June, 7th decision, the importance of specifying, in test and vaccination certificates, which categories of personal data are included in the QR code that is featured.

Germany

Contributor(s): Johannes Struck, Brödermann Jahn Rae GmbH, Hamburg, johannes.struck@german-law.com.

Last updated: 15 October 2020

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	*General Legislation for a tracing tool* The German Law authorises the legislator or the government to introduce a specific tool for data collection against any Pandemic (Sect. 14 of the German Infection Protection Act, modified by Law of 19.5.2020, in force 23.5.2020). The government is empowered to determine the details. **However this law does not mentioned specifically individual tracking tools.** This legislation contains e.g.: - A list of data which can be legally gathered (Sect. 14(2)) - General minimal conditions of the gathering and storage of the data: e.g. pseudonymisation, further access to the data have to be authorised by law (Sect. 14(3)) and possibility of re-identification of the User for serious reasons (Sect. 14(6)). *No specific legislation for a tracing App* As the actual App (see Question 2) is based on voluntary Use, there is actually no project of a specific law (the federal Minster of Justice has taken position on this point as a Law would be unnecessary). The parties which are sitting in the Opposition on the federal level have wished a Law to ensure the voluntary character of the use.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Yes. Since the 16.6.2020, an App named "**Corona Warn-App**" is available to download on iOS and Android devices. *Description* When 2 Users of the App are staying fewer as 2 meter of each other within at least 15 minutes, random generated IDs of the Users (pseudonym) are exchanged between the 2 Apps with Bluetooth. When a User appears to be tested positive to COVID-19, he can share this result (which

		will be also communicated in form of a QR-Code) in his app. His App will then share all the generated IDs to the server, which will share it with all the other Users. The comparison is then made on the App itself. If the shared ID appears in the stored- IDs, the User will receive a Warning, that he was in contact with an infected person – without revealing the identity of this person – and is advised to do a COVID-19 Test. The App gives also a Risk-status (low, 1 risky encounter, high). An actualisation of the status is made every 24 hours. *Developer and provider* The App is provided by the German federal government through the German Robert-Koch-Institute (Federal Agency and research Institute for disease control and prevention; placed under the direct Authority of the Federal Ministry of Health). The App has been developed in cooperation between the Deutsche Telekom and SAP. *Access* First, the gathered IDs are device-stored. The central server has at this moment no access to the stored/encountered IDs. The temporary generated IDs will be shared only with active consent of the positive-tested User and only then be accessible by the so-called Exposure Notification API. It has been insured that the regional Health Agencies (so-called Gesundheitsämter) will not have access to the data. The Users have no access whether to generated nor to the stored IDs. A positive- tested User will not know who received a warning. The Back-end of the App is operated by the Deutsche Telekom. *Acceptance* The App has been voluntary downloaded above 6.000.000 times within the first 24 hours after its availability (as of: 17.6.2020; Source: German Federal Ministry of Health). Over 19.000.000 people have now downloaded the App (as

		of: 12.10.2020). About 1.700.000 COVID-19 Test Results have been shared on the App (as of: 12.10.2020). The Use of the App is however limited by the version of the operating system. The App is only for iOS 13.5 and Android 6.0. *Safeguards* (a) The Users are pseudonymised. The App generates a random ID to each User, which changes every couples of minutes. Each ID is itself based on a random generated key, which itself changes every 24 Hours. A recourse to or identification of the User's real identity is according to the Federal government unlikely. (b) The App is based on the so-called decentralised system. The encountered IDs. are stored on the device (Smartphone). It is only when the User declares being tested positive to COVID-19 that all his generated IDs are transmitted to a central server in order that the information can be transmitted to the all the other Users. The comparison between the "infected"-ID and the stored ID is made on the device of the "end"-User. The device-stored IDs on the device of a positive-tested User will be shared only with his active consent. After 14 days, the device-stored IDs are automatically erased. The providers Apple and Android (i.e. Google) have no access to the data on the App. They only cooperate for Bluetooth-technologies. The government ensured that Huawei, supplier of the Cloud Technology, has no access to the services. Scientists will not have access to the data. (c) The Federal Commissioner for Data Protection and Freedom of Information and the Federal Office for Information Security have been involved in the conception of the App regarding the Data protection aspects. They will be still involved in the further developments of the App.

		The App is open-source to ensure transparency and control made by experts. (d) A “live”-Warning (the app warns if a positive person is in the same place as the user) is not planned and should not be included. *End-date* At this moment (15.10.2020) no end-date of the activity of the App is planned – or at least announced.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	As the actual App (see Question 2) is based on voluntary Use, there is actually no project of a specific law (the federal Minster of Justice has taken position on this point as a Law would be unnecessary). The parties which are sitting in the Opposition on the federal level have wished a Law to ensure the voluntary character of the use. *Companies* Deutsche Telekom: biggest German and European telecommunication company (about 46 Mo. mobile phone Users). Telefonica (at this moment only an offer): present in Germany with the brand O2 (about 43.6 Mo. mobile phone Users). *Data provided* The companies are transmitting the move-flow of the mobile phone Users seen as general population. No individual information is transmitted. *Reasoning* The Companies are cooperating with the Robert-Koch Institute in order to predict and understand the propagation of the virus. It shall help to determine the general behaviour of the population (e.g. staying at home, traveling, etc.). *Access* Besides the companies, only the Robert-Koch Institute has access to the transmitted data. *End-date* No end-date has been communicated.

4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	The App (see Question 2) will still be combined with the actual “paper version”: each customer of a restaurant or a hair-dresser etc. has to give his personal information (name, address, phone number). The communication of this information is mandatory for the use of the service. In the event a customer has been tested positive to COVID-19 When it appears, that a customer has been tested positive to COVID-19, the owner has to contact all the persons who have been at the same time in the rooms. The paper solution will continue. Giving false information exposes the author to fines from EUR 250 up to EUR 1.000 (amount depends of the State).

Hong Kong

Contributor(s): Felix Yuen, PricewaterhouseCoopers Hong Kong, Hong Kong, felix.yuen@hk.pwc.com.

Last updated: 09 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Yes. The measure continues to apply to inbound travellers (regardless of their COVID-19 status). In general but with certain exceptions (such as approved business executives), inbound travellers are subject to a compulsory quarantine, the length of which depends on the place the person returns from and the person's vaccination status, pursuant to the Compulsory Quarantine of Certain Persons Arriving at Hong Kong Regulation (Cap. 599C) (the full regulation here) and Compulsory Quarantine of Persons Arriving at Hong Kong from Foreign Places Regulation (Cap. 599E) (the full regulation here). They are not allowed to leave the place of quarantine. To monitor the quarantine compliance, all persons subject to quarantine are required to install a mobile app called "StayHomeSafe" which comes with an electronic tracker wristband. The wristband uses a geofencing technology to test the strength of the surrounding communication signals like WiFi and GPS, and will alert the authority if the persons try to leave the place of quarantine. The persons must put on the wristband at all times. The Regulations are currently in force, and have an expiry date of 30 September 2021, which may be further extended. The government claims there is no privacy issue (read government publication here). It is said that the wristband and the app only tracks any change of the location instead of the actual location. There is no information as to where the data will be sent to and stored, and to what extent the recipient of the data will use it. Note the requirement of using the app and the wristband is not explicitly written in the

		Regulations. It is implemented as a term of the authority's quarantine order. Separately, the government launched the "LeaveHomeSafe" mobile app for users to keep track of the whereabouts. It is in general voluntary, except for entry to certain venues. Please see question 2 below.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Since November 2020, the Hong Kong government has been promoting the use of a mobile app called "LeaveHomeSafe" to record people's visited locations in public places by scanning QR codes put up at the venues. As the app has raised privacy concerns, the government asserts that: (i) no registration of personal information is required when using the app; (ii) the data will be stored in the user's phone only and not transferred to the government, and will be automatically erased after 31 days; (iii) users will not be required to provide their records to the public authority, unless in the case where the users are confirmed Covid-19 positive. The registration of venues for putting up the QR codes and the use of the app by the public is mandatory in certain cases pursuant to the Prevention and Control of Disease (Requirements and Directions) (Business and Premises) Regulation (Cap. 599F) (the full regulation here). The directions issued under this Regulation are subject to change every 2 weeks, and at the time of writing, dine-in catering businesses, bars and pubs, fitness centres, places of public entertainments, hotels and guesthouses and some other venues are required to put up the "LeaveHomeSafe" app QR codes. Visitors are required to use the app or leave their personal contact details for tracking purposes. Readers are suggest to visit this page for updates.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	There is no public information that private companies are providing such data to the Hong Kong government.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	No.

Hungary

Contributor(s): Dr. András Csenterics, Réti, Várszegi & Partners Law Firm, Budapest, andras.csenterics@pwc.com, Dr. Miklós Klenanc, Dr. Klenanc Miklós Law Firm, Budapest,miklos.klenanc@gmail.com.

Last updated: 14 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	While no explicit legislation has been passed in Hungary as regards contact tracking by means of technology or otherwise, a procedural order (which does not qualify as a source of law) has been published by the chief medical officer, outlining certain rules as regards non-technology focused contact tracking. (Technology-based contract tracking is covered under Question 2.) *Description* As a first step, the appointed officer of the competent governmental bureau (a territorial unit in the Hungarian state administration structure) interviews the infected individual on their potential exposure to COVID-19. If, based on the interview, there is reason to believe that the potentially infected person might have come into contact with other individuals, the authorities contact the individuals in question and further steps are taken, such as additional medical tests and ordering home quarantine. *Status of the legislation* See above (no formal legal effect of the procedure but it is used in practice. Measures taken with regards to infected persons such as ordering quarantine are set forth in the law). *New or existing data* Yes, data gathered by way of the interview with the potential COVID-19 exposed persons. *Access* The governmental bureau and in case of an order, the rules of which are set forth in the law, the minister responsible for public health, the police and medical staff. *Safeguards* No explicit legislation covering the collection of data. However, a

		recommendation by the local data protection authority on the privacy aspects of COVID-related data processing has been published and is widely observed. GDPR and additional Hungarian privacy laws apply. Note however, that mandatory personal data transfers to the minister or the police are covered in effective law and must be carried in case such an order is received. Hungarian laws passed recently have also established an extension for the 1-month deadline set forth in the GDPR for answering data subjects' requests, meaning that the 1-month deadline will start once the special legal regime known as state of emergency (see Question 2) has been withdrawn. Further, during the state of emergency, privacy notices on COVID-related data processing can be provided in a simplified form via websites. *End-date* In general, COVID-19- related laws and procedures will last until the end of the state of emergency, a special legal regime passed by the parliament, providing additional powers to the government in order to combat COVID-19.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	The Governmental Agency for IT Development has introduced VírusRadar, a voluntary application for tracking COVID-19 used on smart phone devices. *Developer* NextSense, which donated the solution to the Hungarian State. *New or existing data* The mobile phone number of the user is processed by the Hungarian State. Otherwise, no personal information is stored, as upon registration, a randomised code is generated and linked to the user's phone number. This code is securely stored in a centralised system and can only be linked to the phone number by

		virologist experts using the centralised system. *Access* The Hungarian State. *Use and acceptance of voluntary measures* Explicit consent of the data subject is collected during the registration procedure. *Safeguards* Apart from the above mentioned, the solution uses Bluetooth to trace possible contacts, therefore no geographic location data is gathered. Further, the phones of users who installed the solution do not communicate personally identifiable information to each other, as encrypted aliases are exchanged, decryptable only by virologist experts using the centralised system. *End-date* N/A, as the application is completely voluntary.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No voluntary offers as mentioned in the question were made, and the affected service providers are under no obligation to carry out data transfers to the government.

4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	The Hungarian data protection authority (NAIH) has issued guidelines on employer data processing in the context of immunity to coronavirus. This is not legally binding, but a wide range of employers have adapted their practices to comply with it. According to the guidelines, the employer is entitled to process only the fact of immunity for the purpose of complying with its obligations under labor law and to ensure that its decisions to implement them are duly justified. Proof of protection against the coronavirus can also be provided by means of a State application (EESZT mobile application). The authenticity of the Immunity certificate and the application can be verified by another State application (EESZT Covid Control).

India

Contributor(s): Dhruv Kakar, S. C. LADI & Co., New Delhi, dhruv.kakar@scladi.com.

Last updated: 9 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	No
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	The answer to item 4 applies here as well. Over the last few months the government has pivoted its stand to make the use of the app voluntary for individuals and private businesses, but it remains mandatory for all government offices and employees.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	If any companies are sharing such data, it is not publicly acknowledged.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	While there is no legislation that has been passed by the government, an app (Aarogya Setu) has been developed and released by the government for the purpose of contact tracing. The use of the app has been a controversial subject over the last few weeks in India due to the data, privacy, lack of transparency, and security concerns. *Voluntary or mandatory?* a. The government and Home Ministry had earlier issued a notification ordering the compulsory use of the app by all public and private employees. This would be an overreach for the government under the relevant IT and disaster management legislations, and would not stand the test of legality in the court.

		b. Please note that India does not yet have a dedicated data privacy and protection law. In December 2019, the government introduced the Personal Data Protection Bill, 2019, but it is still pending before parliament and has not cleared the legislative route towards becoming a law. c. At present, the only data and privacy protection available in India is under Sections 43A and 72A of the IT Act 2000, which give a right to compensation for improper disclosure of information. d. In addition, the mandatory use of the app by private sector employees was ordered earlier, and the organisational heads of companies were to obligated to ensure compliance, which is unrealistic. For ex. The CEO of a company would be legally liable if all employees did not install the app. This position of the government has been rolled back as of last week, and the company management is now required to ensure compliance on a "best effort basis" – vague! e. The app necessarily requires a compatible smartphone. Out of the approx. 1.3 billion people in India, "only" 450-500 million are smartphone users. By and large, rural areas and persons belonging to the lower financial class will not come under the contact tracing initiative. *Data and privacy issues* a. New data is gathered from each user- name, age, profession, address, health conditions, travel history. This data is stored and exchanged with nearby devices using Bluetooth to warn users and record their movements to determine if there has been any contact with COVID-19 positive or vulnerable persons, or persons who have visiting areas that are classified as hotspots or containment zones. This data is also accessible by the developer

		and the government, but the details of the extent of sharing are unclear as the government has not been forthcoming in the privacy policy. b. Health assessment for the app is based entirely on the self-declaration of the user. Therefore, a dishonest user can misrepresent their history or symptoms, without any consequences. c. Privacy policy of the app is very basic, with no details regarding the measures taken for gathering data, processing data, access restrictions, encryption standards, etc. As of date, the privacy policy of the app has silently undergone numerous revisions, each aimed at rectifying or addressing privacy issues raised publicly by citizens, ethical hackers, think tanks, or privacy assessment bodies. While the policy is still not fully transparent by global standards, it is an improvement on the earlier iterations. d. The app code is not open-source, making it impossible for a security or processes audit by independent parties. This is a departure from the usual nature of government apps in India being open-source. e. French ethical hacker “Elliot Anderson” has identified vulnerabilities in the app, and has tried to engage with the Indian authorities to address them. Indian authorities flatly denied any security issues, leading to the hacker to actually demonstrate how he was able to hack into the app and access sensitive health data and location parameters for users inside the PM office, Army headquarters, Home Ministry, etc. The government remained in denial mode, but has silently fixed some issues and made numerous updates to the privacy policy of the app. This exchange is publicly available on Twitter. f. Data is collected through the app using GPS and Bluetooth, leading to an extremely precise location

		tracing for any user. This data is purported to be destroyed once the app is deleted, but this cannot be verified since no further details regarding the use and obfuscation of the data have been made available to the public/user. g. According to the privacy policy, anonymised data may be stored forever. No details have been provided regarding the process and standards for anonymisation or obfuscation. *Current situation* a. With roughly only 40% of the Indian population using smartphones, the efficacy of the app in controlling or monitoring COVID-19 is severely limited, especially considering that classes of people that cannot afford smartphones are also likely to live in areas with high density of population and close proximity. b. We have had numerous queries from clients (private companies) regarding their obligations towards the use of the app by their employees. c. We have always maintained and continue to advise them that the use of the app is not mandatory and any employee has the right to refuse the installation of the app. d. For employers, the “best effort basis” requirement by the government can be fulfilled by advising the employee to install the app, but that cannot be forced on any individual. e. The app has not had the intended benefit or success in the fight against COVID-19 in India. Between September and October, India saw between 80,000 and 100,000 new cases daily, and as of date continues to see over 60,000 daily cases. This is attributed largely to the fact that we are no longer in a state of any real lockdown or movement restriction. Only international flights are restricted, and big businesses and public events are closed or WFH.

		Small businesses, that comprise the majority of the Indian economic landscape, are back to full operations as they have suffered greatly from the economic downturn over the last 12 months, capped off by the COVID-19 impact. *Update 9 June 2021* - As most of the world has noted, the second wave of COVID in India ongoing since April 2021 has painted a grim picture of the devastation caused. The healthcare system has completely collapsed, with upwards of 300k daily new cases seen for a few continuous days at its worst. - There has been an obvious failure of the contact tracing app, which was often noted as being green for many COVID positive people. There is no longer an active initiative by the government or the authorities to promote the use of the app. - Data exchange has been implemented in the COVID testing procedures, with some form of personal state or national ID being required at the time of testing. This enables the state to track individuals who are COVID positive, and also presumably the data relating to location concentration of cases, to enable remedial action. - The Indian vaccination program has been slow, and while technology and data exchange has been extensively implemented, the rate of vaccination remains a concern due to the large population and limited availability of vaccine supplies. - The national ID for every citizen is linked to the central database for COVID (much like the non-mandatory contact tracing app), and vaccination requires online registration. - Similar challenges of access to technology and knowledge for registration are evident in the rural areas and for individuals without

		the means to access the requisite technology. The government also allows registration at vaccination centers, but this is chaotic logistically as people queue up outside hospitals. - The rollout of the vaccination portal was glitchy, and the tech infrastructure behind it failed numerous times due to the sheer volume of users trying to register at the same time. In summary, there has been little or no change in the technology and data aspect of India's fight against COVID. The system has reverted to a more analog model at this time with real people and government authorities taking steps to contain the spread by cordoning off high infection zones, and lockdowns. New Delhi is currently in lockdown since April 17, 2021, and the "unlock" is being undertaken with very small steps at this time.

Italy

Contributor(s): Laura Liguori, Eleonora Curreli, Livia Petrucci, Portolano Cavallo, Rome and Milan, lliguori@portolano.it, ecurreli@portolano.it and lpetrucci@portolano.it.

Last updated: 12 October 2020

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	The Italian government has adopted the Law Decree No. 28 of 30 April 2020, ("**Decree**") establishing a single national platform for the management of an alert system based on contact tracing. It is intended for people who will download, on a voluntary basis, the specific application named "**Immuni**" on iOS and Android mobile phone devices. According to the Decree, such technological solution should have processed users' data until the end of the state of emergency, and in any case no later than December 31, 2020. Then, the Decree has been recently amended by Law Decree No. 125 of October 7, 2020, which extended the period of use of Immuni until the end of the COVID-19 pandemic, and in any case by 31 December 2021. Immuni was officially released on 15 June 2020,after a short "trial period" in which it was available only in a number of Italian Regions. Immuni features a contact tracing system based on Bluetooth Low Energy (the system will use no geolocation data whatsoever, including GPS data) and leverages the Apple and Google Exposure Notification framework. Basically, Immuni allows to record on users' mobile phones a proximity identifier when two users come sufficiently close. If a user tests positive for COVID-19, he/she can communicate his/her health status to the Health authorities and the app and Immuni notifies users who have come into contact with the positive person ("**Exposure Notification**"). Immuni also collects some epidemiological and technical information (e.g. day and duration of exposure, estimated distance between users, information on how contagious the infected user was likely to be when the exposure occurred) for the purpose of helping the National Healthcare Service to provide effective assistance to users.

		In any case, the data collected through Immuni are used solely with the aim of containing the COVID-19 epidemic or, in completely anonymised or aggregated form, for scientific research. Please note that, as clarified also by the Garante, the data processed by Immuni are pseudonymised data rather than anonymous data. The Decree also contains provisions regarding the data governance. Specifically, the Ministry of Health is qualified as the data controller, whereas several public institutions, such as the Civil Protection and the facilities operating within the National Health Service, will act as data processors. Moreover, the Decree establishes various safeguards applicable to the processing of data collected through Immuni: in first place, the data are stored on servers located in Italy and managed by publicly controlled entities. Secondly, the compliance with the principles of the processing (e.g. data minimisation, data protection by design and by default, transparency, and integrity) must be ensured. Lastly, the Ministry of Health has carried out a Data Protection Impact Assessment ("**DPIA**") and submitted it to the prior authorisation of the Italian Data Protection Authority ("**Garante**") according to Section 36 GDPR. Following an in-depth analysis, the Garante has authorised the processing requiring the implementation of some measures to enhance data security and transparency. For instance, users should be informed that the Exposure Notification does not always reflect a real risk of contagion and they should have the possibility to temporarily deactivate Immuni through an easily accessible function. Moreover, according to the Garante, the Ministry of Health should indicate in detail and regularly update the information on the algorithm in the DPIA. The latter should also provide much more accurate information on the processing of the epidemiological and technical information collected by Immuni.

		Following the Garante's observations on the DPIA, in February 2021 the Ministry of Health submitted to the same a modified and integrated version of the DPIA addressing the Garante's concerns. Moreover, such DPIA includes the mode of use of Immuni by Huawei mobile devices and an update of the risk assessment. Furthermore, it also describes how the so-called "Immuni call center" and the "in-app unlocking" features work. Indeed, with respect to the original version of Immuni, nowadays the user who tests positive can initiate the "unlocking procedure" of Immuni – so that the Exposure Notification is sent – either by calling a dedicated call center or by interacting directly with an *ad hoc* section of Immuni. To this end, the user is required to communicate a specific code that uniquely identifies the results of their COVID-19 test, together with the last digits of their social security card (*Tessera Sanitaria*). Furthermore, consistently with the European Commission's work on the interoperability gateway service, the Decree (as amended) allows the implementation of solutions enabling the interoperability between Immuni and other similar European tracking platforms. In October 2020, the Ministry of Health submitted to the Garante an integration of the DPIA necessary to implement such interoperability service which is currently active, as also described in Immuni's privacy policy (available here – ITA only). Finally, under a practical standpoint, in the October 2020 Immuni has been subject to a massive promotional campaign launched by the Ministry of Health and by the newspapers and the downloads increasedsignificantly, reaching 8 million in the same month and more than 10 million in May 2021. However, it should be noted that this data does not reflect how many users actually activated Immuni and/or deleted itafterwards. That said, several diagrams showing statistics on the download of Immuni and its functioning are available at the following link: https://www.immuni.italia.it/dashboard.html.

		On a different note, the Ministry of Health has recently updated the Guidelines for the recovery of economic and social activities, which also provide for contact tracing in relation to certain businesses and events, *e.g*., the list of those present must be kept for 14 days for businesses that offer food, bathing establishments, hotel facilities, cinemas and live shows, swimming pools, hairdressers, beauticians, congresses, fairs, *etc.*
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	The government preferred to adopt a single tracking measure at a national level that ultimately led to the Decree. Indeed, at first it promoted a call for contribution to identify the best digital solution and, then, it set up a task force of experts that identified Immuni as the best tracking solution. However, prior to the government initiative, some regions developed mobile applications to counter the health emergency. By way of example, Friuli Venezia Giulia tested a contact tracing app (which was developed for free by a multinational company and then managed by a company participated by the region itself). This initiative had however to give way to Immuni. Instead, Sardegna released a mobile app that people arriving on the Island could use to facilitate the mandatory self-declaration about their health conditions. A different approach was adopted by Lazio and Sicilia, which released a mobile app to allow users – mainly tourists in the case of the Sicilian app – to check symptoms and get in touch

		with a doctor. Nevertheless, as of June 2021, the Sicilian app seems to be no longer available. Lastly, Lombardy released an application to allow users to fill in a questionnaire, on an anonymous basis, with the aim of obtaining contagion statistics (even though there are some doubts as to whether the data collected by this app would be truly anonymous). Some other regional initiatives have been discussed, but at the moment do not appear to be available, such as the Veneto's mobileapplication to check and monitor users' symptoms. The Garante clarified that the regions cannotlimit access to their territory only on condition that the data subject downloadsand uses a specific mobile application. Indeed, the failure to download an app aimed at countering the spread of the pandemic (whether on a national or a regional basis) cannot lead to any detrimental consequences for the data subject or affect the exercise of his/her fundamental rights, such as, in particular, the freedom of movement. Furthermore, following the spread of contact tracing applications, the Garante clarified that invasive data processing activities, such as contact tracing, can only have an adequate legal basis if they are enshrined in a national law provision, as Immuni.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	Yes. In the first place, on 14 March, 2020, the Italian Telecom Industry Association (ASSTEL) declared that the associated mobile phone providers were willing to make available to the authorities aggregate information derived from the mobility data of all their customers, ensuring in any case compliance with the provisions of the GDPR. These providers themselves volunteered to cooperate with the Civil Protection, the National Institute of Health, the Regions and other authorities committed to fighting the pandemic. For instance, Lombardy used anonymised and aggregated data concerning the "cell tower to cell tower" ("da cella a cella") movements of the mobile phones provided by Vodafone and Tim (two of the major Italian telco providers) to determine how many people were moving around the territory and how they did it. In the second place, Enel X – a company of the Enel Group providing innovative products and services in the energy field – and HERE Technologies – a company providing services related to mapping and location data – published a mobility map. It

		estimates the variation of movements and kilometres travelled by citizens on the national, regional, provincial and municipal territory. The mapping is based on the analysis of anonymous and aggregated data derived from connected vehicles, maps and navigation systems managed by these companies, in correlation with location data from mobile and open data applications of the public authorities. Originally,the mobility map was accessible for free until 31 May 2020, but given the ongoing emergency, such deadline has been extended to 30 June 2021. It can be used to understand the impacts of the COVID-19 containment measures, to identify the areas that need more support in the implementation of these measures, and tomonitor the mobility after the end of the containment measures. In the third place, Facebook, Google and Apple made available to public authorities of several countries, including Italy, aggregated data on users' mobility. This data is obtained, for example, by counting the number of requests for directions received by the relevant applications or by analysing the anonymised mobility data of the social network users.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	Some employers voluntarily implemented tracking measures within the workplace. Nevertheless, in July 2020 the Garante clarified that noother contact tracing apps are permitted, since contact tracing functionalities can only rely on the Decree. Notwithstanding the above, an Italian hi-tech company introduced a system similar to Immuni. The tracking, via Bluetooth, is activated within the company perimeter after the employee has given his/her consent to the installation. Such measures were applied in addition to Immuni and were merely voluntary. For these reasons, the use of these types of apps necessarily relied on the data

		subjects' consent. This however leads to some doubts as to the legal feasibility in the employment context of solutions of this kind, since (as noted by the data protection authorities on multiple occasions) the validity of the consent provided by employees is arguable due to the imbalance of powers existing with the employer. The above-mentioned intervention of the Garante answered to such doubts qualifying the Decree as the only basis to implement a contact tracing measure, also in the workplace. That said, in April 2021 the Government issued a Law Decree introducing the national green certifications (so-called green pass). The latter alternately certify that the person was vaccinated, or contracted COVID-19 and recovered, or had a negative COVID-19 test result. In particular, such certifications are required to enter and exit regions at greatest risk of infection, in case no other reasons justifying the transfer (expressly listed in the Law Decree) apply. The national provisions relating to the green certifications are applicable until the entry into force of the delegated acts for the implementation of green certificates at European level. Such delegated acts will also enable the activation of the National Platform for the issuance and validation of COVID-19 green certifications interoperable at national and European level. Nevertheless, following the above-mentioned Law Decree, the Garante issued an official warning to the Government highlighting major criticalities. Firstly, the Law Decree does not provide a suitable legal basis to introduce and regulate nationwide green certifications. Additionally, it is affected by several data protection shortcomings, *e.g*., the lack of any assessment of possible large-scale risks for the rights and freedoms of individuals, no reference to the data controller, breach of data minimization principle, *etc*. Secondly, the Garante pointed out that such criticalities could have been addressed beforehand expeditiously if the drafters of the decree had opened a dialogue with the Garante

		and requested its preliminary opinion, as required by article 36.4 GDPR. Despite the above, in May 2021, the Government issued a second Law Decree providing for minor amendments to provisions on the green certificates and stating that they will be required to attend parties following civil or religious ceremonies and, potentially, also for other specific events such as shows open to the public, sporting events, trade fairs, conventions and conferences. Finally, there have been initiatives linked to the green certificates at regional level that the Garante has deemed to be in violation of data protection provisions. In particular, the President of the Region Campania has issued an order introducing certifications proving the vaccination, healing, or negative test result of the person as a necessary condition for the use of many services, such as those related to tourism, hotels, wedding, transport and entertainment. In this regard, the Garante has formally warned the region that this system is unlawful because, *inter alia*, it lacks a proper legal basis. Indeed, provisions of this nature, which affect personal rights and freedoms, are admissible only if provided for by a suitable national legislation and not by a regional order.

Netherlands

Contributor(s): Silvia van Schaik, bureau Brandeis, Amsterdam, silvia.vanschaik@bureaubrandeis.com and Chantal Bakermans, Penrose, Amsterdam, c.bakermans@penrose.law.

Last updated: 07 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Yes. On 29 May 2020, the Dutch government submitted a draft emergency legislation for the amendment of the Dutch Telecommunications Act (in Dutch: "*Telecommunicatiewet*"). The draft amendment and more information are available in Dutch. The draft legislation proposal is currently on hold, due to the pending formation of a new government. In addition, the draft legislation has been declared 'controversial' due to privacy concerns. The purpose of the draft legislation is to introduce the obligation for providers of public telecommunications networks and services ("**telco's**") to provide information derived from traffic and location data to the National Institute for Public Health and the Environment (in Dutch: "*RIVM*") for the control of the COVID-19 virus. With this information, the RIVM should be able to better assess the effectiveness of the testing measures and also to act faster in the event of a revival in the number of virus infections. Important to note is that the data to be shared by the telco's concerns 'information derived from traffic and location data'. The derived information entails the total of mobile phones per hour, per municipality, allocated by the derived origin (residential municipality) of the holder of the telephone. In view of the processing of this data, the traffic and location data and the derived origin, will be pseudonymised. In view of the pseudonymisation, technical and organisational measures should prevent the (re-)linking of this information with the respective individuals. The telco's will provide the derived information to the national statistical office, Statistics Netherlands (in Dutch: "CBS") and the CBS will report to the RIVM. In view hereof, the CBS will be considered

		data processor of RIVM. According to the most recent draft legislation proposal, this provision has a temporary character and in principle applies for the duration of six (6) months. However, the draft legislation includes the possibility to extent the provision for subsequent maximum periods of three (3) months. The RIVM and CBS should delete the received information as soon as they are no longer necessary for combatting the COVID-19 virus, and in any event one (1) year after receipt thereof. The Dutch Data Protection Authority (in Dutch: "*Autoriteit Persoonsgegevens*" hereafter "DPA") expressed its concerns in relation to the draft legislation. According to the DPA (i) pseudonymisation does not change the tracking and traceability risk for individuals because linking the derived information to an individual remains possible, (ii) the necessity of processing the data is insufficiently substantiated and, (iii) the proposed security safeguards have not (completely) been taken into account. The considerations of the Dutch DPA in this respect are available in Dutch. The DPA has not yet commented on a more recent version of the draft legislation, possibly because the draft legislation proposal is on hold due to the pending formation of a new government. In addition the Dutch government is working on the development of several digital tools (such as an app) to assist in combatting COVID -19. At first the Dutch Minister of Health, Welfare and Sports indicated that he could not exclude the possibility that apps may be mandatory, because a minimum use is necessary for some apps to be useful. This was heavily criticised by amongst others privacy experts. More recently, the Dutch government corrected this by indicating that the use of such apps shall be voluntary. In this context the Dutch Government launched a contact tracing app,which caused for the introduction of legislative measures. On 6 October 2020 the Temporary Act notification application COVID -19 (in Dutch: '*Tijdelijke wet*

		notificatieapplicatie covid-19') which provides a legal basis for the contact tracing app ("*CoronaMelder*") by amending the Public Health Act was approved by the Dutch Senate. It entered into force on 10 October 2020. The Act provides for a limited list of types of personal data that may be processed, the conditions for such processing and a complaints procedure with the DPA. The text of the Act and related information are available in Dutch. On 30 March 2021 the Temporary Act was prolonged for the second time, until 10 July 2021. On 28 April 2021 the Dutch Minister of Health, Welfare and Sports informed the Government about a fault in the framework of Google Android. The generated codes by which the tracing app ("*CoronaMelder*") works, were stored in the general operating system of the phone and could be viewed by others. Combined with other data sources, this could potentially lead to a violation of privacy. Due to this, the sharing of codes was temporarily stopped until Google Android provided a system update. The sharing of codes and function of the tracing app resumed on 1 May 2021.

2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Yes. As indicated above (Question 1) the Dutch Government has been working on several digital tools including a contact tracing app. The contact tracing app, named "*CoronaMelder*" has been officially introduced on 13 October 2020. The app aims to inform users if they have been in contact with someone who tested positive for COVID -19 and provides recommendations in such situation. More information is available at the Coronamelder website. The use of the app is voluntarily. On 31 January 2021 a report issued by the Ministry of Health, Welfare and Sports on the use of the app was published. The report is available in Dutch. It indicated that 41% of the Dutch population had the intention to use the app, but only 27% actually used it. Research into effectivity of the app is ongoing but the first results indicate that the effect is limited, most likely due to the low percentage of people who actually use the app. Note that prior to its introduction the DPA criticized the app for lack of a basis in legislation, agreements between the Dutch government and Google and Apple and security of the app's servers. Although the lack of legislation is (supposedly) corrected by the legislation discussed above (Question 1), it is not clear if the DPA's other points of criticism have been dealt with. The Dutch government does not promote the use of any other contact-tracing apps that may be available.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No. Telco's initially claimed that under current legislation (in particular the Telecommunications Act and General Data Protection Act) they are not allowed to share traffic and location data with third parties without a legal basis. In view hereof, the government now wishes to effectuate the proposed emergency legislation (Question 1).

		One of the major telco's, T-Mobile, noted earlier that it was asked to provide the traffic and tracking data voluntarily. They mentioned to consider such sharing only if the government was able to guarantee that the traffic and tracking data would be used only for the purpose of COVID-19 research and not, for example, for the purpose of verifying whether individuals comply with the virus prevention measures. According to T-Mobile they did not get such guarantee. Interestingly enough, the current legislative proposal does not explicitly exclude that the derived data will be used for the purpose of verifying compliance with virus prevention measures.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	Although these do not relate to tracking, there are some other relevant legal developments in relation to the use of data and technology in the combat against COVID-19. On 16 April 2021, the Dutch government submitted draft legislation for the temporary amendment of the Dutch Public Health Act in order to introduce the use of test certificates for access to certain events. It was approved by the Dutch Senate on 11 May 2021 and entered into force on 1 June 2021. Official information is available in Dutch only. The legislation introduces the possibility of a requirement of a test certificate prior to allowing people access to specific types of events or locations, such as theatres, sport events and restaurants. The test certificate will include a QR code that is scanned upon entry. The QR code indicated if the person can be granted access based on a negative COVID-19 test result, and in the future on completed vaccination. The process requires two new apps: one for processing a QR code on the side of the visitor of an event ("CoronaCheck") and one for the scanning before entry ("CoronaCheckScanner"). The privacy statement of the "CoronaCheck" app (available in English) states that the QR code will include minimal personal data (only the test result, initials, date of birth and IP address), that will be deleted after the 40 hours have expired. The IP

		address is deleted after a maximum of 7 days. In relation to the draft legislation proposal, the Dutch DPA expressed its concern. The advice is available in Dutch. Moreover, it is interesting to note that the DPA is very engaged in actively sharing information around (potential) privacy issues in relation to combatting the COVID-19 virus. It has created a specific section on its website dedicated to the topic. Unfortunately it is only available in Dutch. The section includes information on: - Privacy and COVID-19 in general; - The use of personal data in relation to vaccination; - The use of temperature and/or health checks; - Quick testing; - Personal data in connection to health checks; - Privacy of students in connection to home-education; - Privacy in the workplace (incl. remote working). The information provided demonstrates that the DPA takes a rather strict approach. For example, it holds that checking someone's temperature in this context is probably only permitted with theconsent of the data subject and that such consent will generally not be obtained freely and thus will not be considered valid(for example in employment relations). It also questions the effectiveness of measuring temperatures. Moreover, it indicated that while in some situations health checks may be performed, the results may not be registered.

Slovakia

Contributor(s): Štěpán Štarha and Adam Kližan, Havel & Partners, Bratislava, stepan.starha@havelpartners.sk and adam.klizan@havelpartners.sk.

Last updated: 03 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Yes, the National Council of the Slovak Republic adopted Act No. 242/2020 by which the following legislation have been changed. The first is the Act No. 351/2011 Coll. on electronic communication as amended providing the legal scope for tracking individuals by (i) obtaining data from mobile communication providers ("The First Amendment") and the second is Act No. 355/2007 (ii) the use of mobile app ("The Second Amendment"). *The First Amendment* - Based on The First Amendment, the Public Health Authority of the Slovak Republic ("PHA") was entitled to request the provider of electronic telecommunication networks and services to provide existing data to extent of name, surname, phone number, address and location data of user of electronic telecommunication networks and services based on the reasonable written request submitted by the PHA and with the written consent or otherwise credibly verifiable consent of the concerned person. - Based on the latest update, the PHA is allowed to request in written form from the electronic telecommunication provider either the data to the extent of telephone number, localisation data and operation data of the data subject even without the data subject´s consent. - The processing of data of data subject without his/her consent can be performed solely in case of data subject, who arrive to the Slovakia from the countries that are not included in the list of less risky countries which is regularly updated by the Ministry of Foreign and European Affairs of Slovak

		Republic. Such processing may be carried out by PHA for period of 60 days from the day of their receipt by the PHA, after that the data have to be destroyed. - The data could be processed only by the PHA. - As regards to the safeguards, the data shall be processed:in anonymised form for statistical purposes which are necessary for the precaution, prevention and creation of a model of the development of threats of life and health; o for the purposes of identification of recipients of text messages who shall be informed about the specific measures of the PHA in order to protect life and health; o exclusively to the extent necessary for identification movement of the concerned users of electronic telecommunication networks and services in order to protect life and health. - Please note, however, that the PHA is no longer entitled to collect, process or renew data, although this legislation is still valid (the statutory period for such data processing ended on 31 December 2020). To the best of our knowledge, the renewal is not planned. A review of the data collection by PHA will be subject to control of Data Protection Authority in 2021. *The Second Amendment* - The Second Amendment regulates in particular the use of (i) the app on monitoring of ordered isolation (eQuarantine) and (ii) the app on monitoring of a contact of the mobile device with other mobile devices during the mandatory isolation ordered by the state authorities. Given the purpose of this amendment, the individual to whom a mandatory isolation was ordered, shall be entitled to opt for

		self-isolation instead of the - institutional quarantine, if this person provides consent with the use of the app on monitoring of the ordered isolation (note that the app on monitoring of the contacts of the mobile device with other mobile devices can be used voluntarily). After the consent was provided, such person shall be obliged to comply with other statutory requirements, e.g. to allow the app with an access to the camera, nonstop internet connection, to allow localisation data, smartphone shall be permanently switched on during self-isolation etc. More information on eQuarantine is available here (in English). - eQuarantine was developed by volunteers for free. Currently, eQuarantine is available for Android and also for Apple. - eQuarantine as well as the app on monitoring of the contacts of the mobile device with other mobile devices are operated by the PHA. - The PHA shall be entitled to process new data to the extent prescribed by The Second Amendment (in particular name and surname, identifier of the app, unique code of the app, the place in which the home isolation is ordered and other associated information in this regard, location data, national identification number, information on the compliance or non-compliance with ordered home isolation, mobile number, information related to the health etc.). Relevant legal safeguards have been adopted, e.g. data processingvia the apps shall be supervised bythe Data Protection Office of the Slovak Republic which shall be obliged to undertake a specific inspection, retention periods were implemented, DPA shall be conducted by the PHA etc. - The data could be processed for the period necessary to achieve the statutory purpose, however, by 31 December 2020 at the latest. - As far as the state quarantine has

		been replaced by individual home quarantine and testing after the arrival from the countries which are not listed as less risky countries, the eQuarantine app is no longer used, even if the pertinent Act is still valid. Please see also our comments concerning recent registration obligations in question 4 below.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Yes, some of the technological measures described above are recommended (collection of data with the data subject´s consent) and repeatedly promoted by the Slovak government. This conclusion also naturally stems from the fact that both pieces of legislation were adopted based on the governmental proposals.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	We are not aware of any companies which would voluntarily provide such data to the Slovak government in order to track individuals. However, certain level of cooperation between the mobile phone providers and the Slovak government could have been observed as regards to the text messages which are sent to the individuals entering Slovakia from abroad. By this way, relevant persons are informed in particular about the obligations ordered by the governmental measures as regards to the COVID-19 as well as on potential sanctions in case of non-compliance with applicable restrictions.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	Effective from May 2021, new registration obligations concerning persons travelling from abroad to Slovakia are applicable: - registration on the governmental website korona.gov.sk when entering Slovakia at the latest; - during their stay in the territory of Slovakia, these persons are obliged to prove their compliance with registration obligation (above) to a member of the Slovak Police Force if requested; - in addition, persons entering Slovakia by air transport are also obliged to fill in the Public Health Passenger Locator Form in connection with the protection of public health published on the website of the Ministry of Health of the Slovak Republic.

Spain

Contributor(s): Cristina Hernandez-Marti Perez, Hernandez Marti Abogados, Barcelona, cristina@hernandez-marti.com.

Last updated: 16 October 2020

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	*Description* *Geolocation system. DATACOVID-19* *Status of the legislation* Already implemented. *New or existing data* It is provided by the telecom companies to the Statistics National Institute. *Access* The Statistics National Institute is responsible of the data treatment and the telecom companies are in charge of the data treatment. *Safeguards* Aggregated and anonymised data will be collected in accordance with Regulation 2016/679 and Spanish Act 3/2018. *End-date* Ended when state of alarm ended.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	RADAR COVID: It is an app that the citizen can download on a voluntary basis and can notify if they are positive in COVID- 19. The General Secretariat for Digital Administration has been developing, with the knowledge and agreement of the Ministry of Health, an application for contact traceability in relation to the pandemic caused by the COVID-19 called "COVID Radar". In July 2020, with the agreement of the Ministry of Health's Directorate-General for Public Health, Quality and Innovation, the SGAD successfully carried out its pilot project, the success of which guarantees the viability of the proposed solution for tracking close contacts. The Ministry of Health and the competent Regional Ministry of Health of the Community concerned "will appear as the

		persons responsible for the processing of personal data and the SGAD as the processor".
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	*Companies voluntarily providing data* All the telecom data. *Data provided* Movement of all the devices, without identifying the devices. Before, during and after COVID-19 situation. *Reasoning behind providing the data* The aim is to protect the Health and Safety of citizens as well as to offer additional channels of information. Also to have real information on citizens´ mobility that will have an impact on the hospitals capability in each region. *Access* Statistics national institute. *End-date* Ended when the state of alarm finished.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	N/A

Sweden

Contributor(s): Anna Eidvall and Maria Jennerholm, MAQS Advokatbyrå AB, Gothenburg, anna.eidvall@maqs.com and maria.jennerholm@maqs.com.

Last updated: 03 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	No, the Swedish government has not introduced any legislation aimed at tracking individuals and identifying people they have come into contact with due to COVID-19. To date, the Public Health Agency of Sweden has determined that it would not be effective to use such technology, which has been respected by the Swedish government. However, this may change in the future. On 4th January 2021, the government passed a new temporary legislation on how to deal with COVID-19, but it does not cover tracking of individuals.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	No, the Swedish government has so far not recommended or promoted the voluntary use of technology measures to track individuals and identifying people they have come into contact with. However, the Swedish Public Health Agency has in a report defined tracing and testing as two of the most important measures to combat the spreadof COVID-19 during 2021 and stated that they are positive to the use of anonymized data for tracking in relation to COVID-19.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No, but the Public Health Agency of Sweden is obtaining anonymised and aggregated data from the network operator Telia about its Swedish customers, for the purpose of analysing if they follow the Swedish government's recommendations in connection with the spread of COVID-19 (e.g. limit domestic travels). Also, a number of suppliers have offered to develop different kind of apps to track and monitor the virus, either by the use of geolocation data or data on symptoms. One supplier have also offered to rebuild the chain in the pandemic management system. It should also be noted that researchers at Lund University in Sweden have launched a free app to help map the spread of infection in Sweden and increase knowledge of the coronavirus. The app's ambition is provide decision makers with

		valuable insight into how contagious the virus is and what drives its spreads.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	The Swedish Data Protection Authority has issued guidance on personal data and COVID-19 (which includes guidance on what types of information constitute health related data and what employers should consider when processing employee personal data when combating the virus), digital infection tracking and digital teaching. In addition to the guidance, it has also published answers to frequently asked questions on the subject. The Swedish Work Environment Agency has issued guidance regarding work environment risks relating to COVID-19, e.g. due to increased work from home.

Switzerland

Contributor(s): Janine Reudt-Demont, Niederer Kraft Frey AG, Zurich, janine.reudt-demont@nkf.ch and Kaj Seidl-Nussbaumer, Probst Partner AG, Winterthur, kaj.seidl-nussbaumer@probstpartner.ch.

Last updated: 12 October 2020

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Yes, on Federal level, Switzerland has introduced legislation aimed at tracing individuals by use of an app or similar means on a voluntary basis. Additionally, Switzerland has introduced legislation aimed at tracing individuals returning to Switzerland from countries or cities/areas with high infection rates on a mandatory basis. Unlike the voluntary use of an app as described below, this tracing is executed with a low-tech approach, i.e. with calls made based on flight itineraries, border controls, self-declaration and similar measures. On state level, some cantons have introduced legislation aimed at tracing of individuals on a mandatory basis by use of contact details provided by those individuals in specific situations. For more information on this, please refer to Question 4. On 19 June 2020, the Swiss Parliament has adopted legislation (Art. 60a of the Epidemics Act) to allow the Swiss Government the operation of the Swiss PT-App ("PT" stands for "Proximity Tracing"). The Swiss PT-App, often also referred to as the "SwissCovid App", has been launched for use by the general public on 25 June 2020. Use of the Swiss PT-App is voluntary. *Purpose* During the current state of fighting the COVID-19 pandemic, an important measure is the tracing and interrupting of infection chains. The launch of the Swiss PT-App is aimed at supplementing such tracing already practiced at the start of the pandemic (and as still ongoing) by cantonal authorities via telephone calls.

		The Swiss PT-App was created by two leading Swiss universities (namely the EPFL and the ETHZ) in collaboration with the Federal Office of Public Health (FOPH). The necessary backend (server) IT-system was developed and is operated by the Federal Office of Information Technology, Systems and Telecommunication (FOITT) on behalf of the FOPH. *Operations and functions* The Swiss PT-App functions as follows: - Recording of contacts: The Swiss PT-App is an application software installed on the smartphone (with either the latest version of iOS or Android as operating system) that can be downloaded from the app store. For such download, no personal information such as phone number, name or e-mail address is required. At installation, a random initial encrypted ID is generated. After installation, the smartphone sends out encrypted IDs via Bluetooth (Low Energy). These are long, random and daily changing character strings that do not contain any information on the person using the app, such person's location or the kind of device used. If another smartphone, on which the same Swiss PT-App is installed, is less than 1.5 meters away for a total of more than 15 minutes on end, the devices exchange their encrypted IDs. This creates a local list of encrypted IDs received from devices that the person has been close to for a longer time and so registers the epidemiologically relevant encounters. Users do not have to enter or change any settings, but must simply and only carry their smartphone with them with the Bluetooth function turned on. After two weeks, all encrypted IDs collected are automatically deleted from the device. As long as no infection is notified by the user (see below), no data are centrally stored within the PT-system.

		- Notification mechanism: If a Swiss PT-App user tests positive for COVID-19, he or she receives a so-called "Covidcode" from the cantonal medical service, whereby the code is created via the FOPH's website and via the backend-server operated by FOITT respectively. This step is important to prevent abuse, as the app's notification function can only be activated by the user with this Covidcode. After such activation, which is entirely voluntary, the other app users are automatically – by retrieving the relevant information via the backend-server – informed that they had close contact with a person who tested positive and that they themselves may be infected. The notified persons only receive information on the date, but not on the time or place of the potentially infectious contact. Due to the encrypted and changing IDs, this information is generated anonymously, i.e. neither users, nor the federal authorities hosting the application on their server will know who the infected person is and the privacy of users is guaranteed throughout. Now the informed user can contact the hotline mentioned in the app and clarify the next steps (e.g. quarantine, testing, treatment etc.). In summary, the Swiss PT-App does not collect any personal data, location data or motion data of the user. The contact data (i.e. the exchanged encrypted IDs) are also not centrally stored, but only locally on the respective devices. Consequently, the Federal Data Protection and Information Commissioner (FDPIC, i.e. the Swiss National Data Protection Authority) as well as the National Ethics Committee have approved of the use of the Swiss PT-App. The Swiss PT-App has only been designed to fight COVID-19 and as soon as the app is not needed anymore for this purpose, it will be discontinued and all data will be deleted.

		Use of data for statistical purposes Certain anonymous data, such as (i) the number of generated activation codes (Covidcodes) per canton, (ii) the number of calls to the specific hotline for the informed users, and (iii) the number of app downloads from the Apple or Google store are used for statistical purposes. *Necessity of legislation* Federal bodies that systematically obtain data from a large number of personal sources, such as mobile phones, and process it automatically must, in view of the associated risks to privacy and informational self-determination, be able to base themselves on a legal basis within the meaning of Article 17 para. 1 of the Swiss Data Protection Act (DPA). This requirement also applies if the use of the app is voluntary. Consequently, despite the voluntary use of the Swiss PT-App, the implementation of respective legislation was necessary, as the Swiss PT-App's backend is integrated into the FOITT's infrastructure. Furthermore, the FOPH is responsible for the operation of the app and qualifies as controller of the data file in the sense of the DPA. *Content of legislation* The legislation, which consists in an urgent adaptation of the existing Epidemics Act, authorises the FOPH to operate the Swiss PT-App, regulates the basic principles of the app's purpose and functions as well as the purpose of the data processing connected therewith (all as described above). In addition, it contains a prohibition of discrimination or preference based on participation or non-participation in the PT-system, so that the principle of voluntary participation and the right of informational self-determination are preserved. The legislation further provides that the operation of the PT-system may only last as long as is necessary to fight the COVID-19 pandemic. It also authorises the Federal Council to conclude agreements with other states with regard to the interoperability of similar systems. Further, a right of users

		who have been informed via the Swiss PT-App of an encounter to take a COVID-19 test for free (costs borne by the Swiss Federation) as well as the possibility to discontinue the Swiss PT-App in case it proves to be ineffective has been adopted. The details on the Swiss PT-App's operation are regulated in a separate implementation ordinance (Ordinance on the Proximity-Tracing System for the Coronavirus Sars-CoV-2). *Swiss PT-App as medical device* With the technical implementation as outlined above and in particular with regard to the health-related recommendations provided, the Swiss PT-App qualifies as medical device under Swiss law. According to the Federal Council's dispatch for the attention of the Swiss Parliament with regard to the legislation to be implemented ("*Botschaft*"), the Swiss PT-App fulfils all respective regulatory requirements under the Therapeutic Products Act.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	Yes, the use of the Swiss PT-App is voluntary but recommended. The Federal Council promotes the use of the Swiss PT-App, inter alia by way of a mass media campaigns (TV-spots, banners etc.). According to a survey conducted at the end of April 2020, 70% of Switzerland's population was in favour of the introduction of a PT-app. Most of the questioned persons confirmed that they were likely to install and use the app themselves. On its first day (25 June 2020), the app has been downloaded 150'000 times. Today (October 2020) and according to numbers published by *statista* (website last visited on 12 October 2020), however, it is clear that the SwissCovid App is only actively used by around 1.6 million people. I.e. only around 18.5% of the Swiss population have downloaded it and have Bluetooth activated. For more information on the app and its functions, see answer to Question 1.

3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	No. However, Swisscom, the state-owned and largest Swiss mobile phone network provider, had provided the FOPH with certain information about the mobility of the population and size of local gatherings throughout the COVID-19 "lockdown". The purpose of this information was to enable the FOPH to ascertain whether the Federal Council's prohibition of gatherings of more than 5 people at the time had generally been adhered to. This information was not shared entirely voluntarily, as the FOPH had issued an order based on the Epidemics Act obliging Swisscom to grant access to its pre-existing Mobility Insights Platform (MIP). Swisscom and the FOPH both stated that no personal data was disclosed to the FOPH, but still the cooperation was subject to critical media coverage. Due to these media reports, the FDPIC started a summary enquiry, the results of which can be accessed here in in German. The FDPIC came to the conclusion that Swisscom (and the FOPH) had rightfully stated that only anonymised data was shared with the FOPH. In particular, it held that: - localisation data had been pseudonymised as early as possible by hashing and subsequent aggregation; - no organisational measures had been described, but that there was no reason to believe that there were obvious deficiencies, since the product (MIP) had been in operation for a number of years; - Swisscom made available statistical and visualised information to the FOPH, but none of the non-obfuscated ("*Klardaten*") or pseudonymised data that underlied the MIP; and - the data made available to the FOPH had been anonymised. However, the FDPIC criticised that information to the public about the cooperation had been scarce and not easily found, which is why he requested Swisscom to make available detailed information about the data processing

		underlying the cooperation. Swisscom had complied with that request and issued an FAQ, detailing the FOPH's access to the MIP. The FAQ is available here in German. Additionally, the FOPH had released a media statement, which inter alia showed what the visualisations it received looked like. This statement is available here in English.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	As mentioned above, several cantons have implemented legislation aimed at tracing individuals based on contact details which have to be provided by those individuals in specific situations. For example, in the canton of Zurich, restaurants are obliged to request contact details from their customers (name, first name, zip code, mobile number, e-mail address, time of entry and leaving of the establishment) to enable the cantonal authorities to trace such customers in case of an infection of another person who was present at the restaurant at the same time. In the case of dance clubs, the clubs also have the obligation to verify the mobile phone number.

Taiwan

Contributor(s): Sophia Yeh, Tsar & Tsai Law Firm, Taiwan, sophiayeh@tsartsai.com.tw.

Last updated: 09 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	Yes, according to Taiwan Communicable Disease Control Act and Taiwan Personal Data Protection Act, Taiwan implemented a phone tracking system “electronic fence”that uses location-tracking to ensure people who are quarantined stay in their homes. The competent authority may ask the individuals to provide their mobile phone numbers or ask them to carry the provided mobile phone during the 14 dayshome quarantine. For those subjected to a mandatory 14 days home quarantine, the use of such designed technological measure is compulsory under Taiwan laws.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	In May 2021, Taiwan's Central Epidemic Command Center (“CECC”) launched the “Taiwan Social Distancing” app (the “App”) to prevent community transmission of Covid-19. By using Bluetooth technology, the App generates and saves de-identified random IDs in each user’s own device when users have close contact (e.g. less than two meters for two minutes.) Users could upload their random IDs voluntarily when tested positive of Covid-19; then the App would base on the ID received to notify other users who have contact with him over the previous 14 days. Besides, the CECC uses vouchers as incentives to encourage people downloading the App and uploading their random ID if tested positive. Further, Taiwan government also introduced the “contact tracing text messaging service”, which allows individuals to use their mobile phones to leave contact information when visiting stores, markets, government buildings and public transportation venues. Business owners who wish to use this service should first apply for a QR code and an identification code.

		The individual could either use a QR code reader to generate a link to send a message to 1922 (the Covid-19 hotline) or direct text the identification code to 1922 when entering the venue. According to the CECC, the text would be free of cost. This service records the time and the place which the individuals visit, helping the CECC to track confirmed cases and people in contact with them. Also, It would be faster and easier for business owners to follow the Guidelines for the Contact-Based Policy, and the personal data of customers could be better protected since the data is not accessible to business owners. Due to the Covid-19 outbreak, Taiwan government also urged public transport passengers to register their E-tickets for better epidemic control. A registered-card with the name and the telephone number of the user could help the CECC to better trace and notify people when needed.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	Under Taiwan laws, Taiwan government is entitled to receive the specific data from the country's major telecoms companies to track the location of the quarantined individuals, for example, the telecoms companies can provide the government the cellular location data of their users to assist the tracking of confirmed cases and people in contact with them (potentially infected individuals). As for the data collected by the App, the random IDs are stored only in the user's device unless the user tested positive voluntarily uploads his random de-identified ID. The data provided by individuals in the contact tracing text messaging service is stored at the telecoms companies, and would only be used for epidemiological investigation. The data would be deleted after 28 days pursuant to agreements between the telecoms companies and the CECC. As for the E-ticket system, it is legitimate for the e-ticket companies to provide the competent authority the personal data stored in e-tickets and their systems for

		epidemic control.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	N/A.

United Kingdom

Contributor(s): Chloe Taylor, Carpmaels & Ransford, London, chloe.taylor@carpmaels.com and Zoe Walkinshaw, Bristows, London, zoe.walkinshaw@bristows.com.

Last updated: 18 June 2021

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	UK government started "test and trace" scheme on 28 May 2020. A contact tracing app proposed by the NHS digital innovation unit was tested on the Isle of Wight in May 2020 but the app could not be used due to restrictions Apple imposes on how Bluetooth is used by third-party apps. There is now an official NHS app which uses an Apple-Google solution. For further background on the app, see below. UK university Kings College London also developed an app which tracks COVID-19 system and which has been downloaded by over 4 million users. *Test and trace* - there are two types of Covid testing in the UK: PCR tests – mainly for people with symptoms, these are sent to a lab to be checked; and rapid lateral flow tests – these are only for people who do not have symptoms, and give a result in 30 minutes using a device similar to a pregnancy test. Both can be obtained from the UK government free of charge. The contact tracing app was originally developed by the NHS technology team based on a centralised database. This was a bespoke system without collaboration with Google or Apple. The original app was intended "not to store any personal data". Of course, it collected health data from users, but the NHS claim was based on the fact that it was not necessary to enter name or address information – it did however collect location data.

		As of 18 June 2020, it was announced that there were significant problems with the app – specifically it could not recognise the vast majority of Apple devices (c. 96%). As a result, the NHS stopped developing this version of the App and switched to a version based on the Google and Apple developed platform (as in the cases of the German and Italian Apps). Further details can be seen here. *Status of the legislation* No legislation yet in force, aside from existing privacy legislation. *New or existing data* New data gathered, either via tests and follow up, or via NHS app. *Access* Contact tracing/public health teams, the NHS and the government. Not yet clear who else may have access. *Safeguards* No legislation yet in force, but DPA 2018 and GDPR provide protections. *End-date* Not yet clear.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	See above (Question 1).
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	Mobile phone operators and tech companies have been discussing how to work with the government to tackle COVID-19, but it is not yet clear what the outcome of those discussions has been, or what data (if any) companies would be willing to provide to the government.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	None.

United States of America

Contributor(s): Katja Garvey, Kegler Brown Hill + Ritter, Columbus, Ohio, KGarvey@keglerbrown.com.

Last updated: 20 October 2020

	Question	Answer
1	Has your jurisdiction introduced any legislation aimed at tracking individuals (either by use of an app, by obtaining data from mobile communication providers or otherwise) and identifying people they have come into contact with? Or is the government in your jurisdiction planning to do so?	No. Please keep in mind I work in Ohio, other states might have done so, but I am not aware any have implemented anything along those lines.
2	Has your government recommended or promoted the voluntary use of technological measures to track individuals and identifying people they have come into contact with?	No. Please keep in mind I work in Ohio, other states might have done so, but I am not aware any have implemented anything along those lines.
3	Have any companies in your jurisdiction storing movement and/or communication data (e.g. mobile phone providers) voluntarily offered to provide data to your government to enable the tracking of individuals and identification of people they have come into contact with?	Not that I am aware of. Please keep in mind I work in Ohio, other states might have done so, but I am not aware any have implemented anything along those lines.
4	Are there any other relevant legal developments in your jurisdiction regarding tracking individuals in relation to combatting COVID-19 you would like to share with us?	No.

International Association of Young Lawyers
Association Internationale des Jeunes Avocats

Avenue de Tervueren 231
1150 Brussels Belgium
T: +32 2 347 33 34
www.aija.org