CORONAVIRUS AND CONTACT TRACING APPS

Global Privacy Perspective

ADDLESHAW GODDARD

Illustration: A world of complexity by Sam Hadley

TRANSPARENT, TEMPORARY, ANONYMOUS: WILL THE CORONAVIRUS TRACING APPS OVERCOME DATA AND PRIVACY CHALLENGES IN EUROPE?

> **While the war against COVID-19 has ignited unprecedented tech innovation to eradicate a flu-like disease caused by the novel coronavirus, the access and use of health and location data of millions of individuals raise legitimate concerns of equally unprecedented mass surveillance of society at large.**

As the COVID-19 (coronavirus) outbreak has prompted a wide range of responses from governments around the world, contact tracing apps have emerged as a double-edged digital weapon, both as a containment measure and as a privacy challenge. While the war against COVID-19 has ignited unprecedented tech innovation to eradicate a flu-like disease caused by the novel coronavirus, the access and use of health and location data of millions of individuals raise legitimate concerns of equally unprecedented mass surveillance of society at large.

On either side of the Atlantic, the race to develop coronavirus contact tracing apps seeks to urgently help understand the spread of coronavirus and reduce the pressure on national health services by allowing individuals to more accurately monitor their exposure to the virus. Contact tracing is a well-known tool to tackle epidemics, and has traditionally been done manually. In this era of Big Data, digital tracking apps provide a highly effective tool to detect risky contact events and provide information against the spread of Covid-19 by giving access to screening tests and instigating quarantines. From an epidemiology perspective, it is not yet entirely clear how wide an impact these tracking applications will have on the spread of the epidemic, given that these apps are to be used on a voluntary basis.

The purpose of these contact tracing tools is to assist with the easing out of lockdown by tracing contacts that lead to infections and break the contamination chains as early as possible. Individuals that may have been in close contact with the virus will be identified and automatically notified so they can start self-isolating or get tested. App users' location data can help devise the most efficient models to assess the spread of the virus and the overall effectiveness of confinement measures

In early February 2020, contact tracing technology was first launched in China as a way of containing the spread of the virus from Wuhan with a color-coded app — green, yellow or red — that tracks individuals and indicates their health status. Equivalent initiatives were quickly replicated with nuances in South Korea, Singapore, India and Australia. The United States of America and New Zealand are ready to follow shortly. In Europe, about eleven countries have already launched their own versions of contact tracing apps and many more are expected to quickly follow suit, including the United Kingdom and France.

In this article, we will be looking at the privacy challenges raised by the contact tracing apps and how implementing privacy fundamentals as part of the development of those apps may win public trust and convince people to embrace this new technology.

SECTION 1

Explores the general approach to the apps by different countries globally. It should be noted what is acceptable in the name of public health may vary from country to country subject to the applicable privacy laws.

SECTION 2

Looks at the European approach in more detail, with a particular focus on compliance with the existing data and privacy protection legal framework in the UK, France and Germany.

SECTION 3

Sets out some brief conclusions and provides a table that we compiled as a reference point for the main European privacy-centric initiatives and recommendations published to date.

1. GLOBAL APPROACH: PRIVACY VERSUS MASS SURVEILLANCE

According to researchers from Oxford University's Big Data Institute, at least 60% of the population in a country would need to download such apps in order to achieve the so-called "digital herd immunity" and put an end to the spread of COVID-19. However, concerns over privacy and security implications of such contact tracing apps are widespread globally, with significant attitudes of mistrust over the intrusion and misuse of 'Big Data' prevalent in western democracies. These concerns have perhaps been stoked by the well-publicised state surveillance measures that have been taken in Asia when rolling out such apps, many of which have been condemned as intrusive, with particular disquiet around China's 'Health Code'.

Clearly, this crisis has unveiled new thoughts on how far public interest grounds can be stretched by governments and their sponsored apps to process health data at scale when the processing of such data is key to saving lives.

A. CHINA'S HEALTH CODE APP

The health code service made available to citizens of the PRC requires registration on one of the ubiquitous platforms developed by Alipay or WeChat for the Chinese government. For registration purposes, basic information is required at first then further queries on health status and travel history are more invasive of privacy, as users are then asked to identify any close contacts diagnosed with the virus. The app provides users with colour-coded designations precisely based on their health status and travel history, and a QR code that can be scanned by authorities.

Although, the apps work differently by city and province, a person identified under a green code would generally be allowed to travel freely around China. A yellow code would require self-isolation while a red code would alert the user of being a confirmed Covid-19 patient subject to quarantine.

The coronavirus crisis has brought to light the extent of China's surveillance state powers and its ability to redirect its mass surveillance network to efficiently track people in the fight against the virus. The lack of information provided to citizens on how the apps work and what data is stored reflect the general approach. The data sharing arrangement between the two tech giants and government agencies is no less a concern and no explanation was provided on why the information collected through the apps may be shared with some state services unrelated to the fight against the virus.

Overall, China's successful apps are down the pervasive use of smartphones amongst the population and the unfettered access and data sharing of user's data between the tech giants and the government.

However, there is growing trepidation that these apps may not only trigger serious breaches of privacy and data security but that they may also be setting a troubling blueprint for new forms of automated social control that could persist long after the pandemic eases off.

Thoughtful and targeted legislative efforts, like this bill, will address specific consumer privacy violations resulting from COVID-19.

Senator Moran

B. UNITED STATES' CONTACT TRACING PROJECTS

Many State governments, private enterprises, and academics across the US have disclosed plans to develop contact tracing technology to help contain the COVID-19 pandemic. Washington has largely left it to private initiatives and, in particular, academics to lead the charge.

In this respect, academia has kept privacy considerations at the core of their considerations in the development of their contact tracing projects. MIT pioneered with the Safe Paths app. It is a multi-faculty, cross-MIT effort, in collaboration with institutes including Harvard University, Stanford University, and the State University of New York at Buffalo; clinical input from Mayo Clinic and Massachusetts General Hospital; and mentors from the World Health Organization, the U.S. Department of Health and Human Services, and the Graduate Institute of International and Development Studies.

The Safe Paths app (PrivateKit) uses overlapped GPS and Bluetooth trails that allow users to know if they have been in contact with someone diagnosed positive for the virus, by matching location data on users' devices with anonymised location data of infected patients. In this way, the app maintains the privacy of both the user and the diagnosed infected patients. Users remain in control of their data stored in their devices. Data sharing between Covid-19 patients and health authorities is on an opt-in basis.

Another initiative led by the Stanford University and the University of Waterloo has devised a contact tracing app called Covid Watch based exclusively on Bluetooth signals.

Unlike the European Union which has adopted the GDPR, the United States are still discussing a potential new federal privacy law which would have impacted the development of contact tracing technology. However, the apps still need to comply with a number of strict privacy and security requirements both at the federal and state level.

In particular, at the federal level, privacy and security rules applying to the health sector set out under the Health Insurance Portability and Accountability Act (HIPAA) should apply to contact tracing projects if the teams involved in the app developments or management qualify as regulated "covered entities", such as the healthcare providers and other related players. This is not to disregard the importance of significant privacy and security laws implemented by a great number of US states which may equally impact such apps, such as the California Consumer Privacy Act (CCPA) which came into force on the 1st January, 2020. The CCPA grants expansive consumer privacy protections through new data privacy rights.

It is worth noting that a group of four Republican Senators plans to introduce a privacy bill that would regulate the data collected by coronavirus contact tracing apps. The so called COVID-19 Consumer Data Protection Act would *"provide all Americans with more transparency, choice, and control over the collection and use of their personal health, geolocation, and proximity data,"* according to a joint statement. It is contemplated that state attorneys general will enforce the Act.

"As Congress seeks to enact a uniform comprehensive data privacy and security framework, thoughtful and targeted legislative efforts, like this bill, will address specific consumer privacy violations resulting from COVID-19," Senator Moran said in a statement.

The bill will require organisations to obtain express consent from individuals if personal data about their health, location or proximity to another person is collected. They will also be required to disclose the uses, retention and deletion period of the data and to implement specific measures to ensure that no re-identification of individuals may be possible on the basis of anonymised data.

C. THE EU AND THE UK CONTACT TRACING APPS: CENTRALISED VERSUS DECENTRALISED?

In contrast to China's contact tracing model based on the use of location data, the EU and the UK have had to build into its contact tracing technology solutions the concept of privacy by design, and have had to comply with all applicable privacy and data protection laws.

In the EU, most of the Member States favour short-range Bluetooth connections or "handshakes" between mobile devices to register a potential contact, without tracking physical location using GPS and therefore using location data. However, there is widespread disagreement between choosing to log such contact events on the individual devices or on a central server.

Therefore, two distinct and competing models of contact tracing technology are dividing the EU. These are the 'centralised' versus the 'decentralised' approaches.

On one side, a group of countries initially led by Germany champions the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT https://www.pepp-pt.org) which recommends the 'centralised' approach. Composed of a consortium of over 130 members, including telecommunications operators, health service providers, scientists and other relevant actors and stakeholders, this initiative launched on 31 March 2020in order to develop and offer an EU data privacy and data protection compliant tracing technology that could also be effective in the fight against the spread of COVID-19. The opponents to this approach, backed by Switzerland, Austria and Estonia favour a 'decentralised' contact tracing protocol called DP-3T that would be supported by the technology alliance formed between Apple and Google.

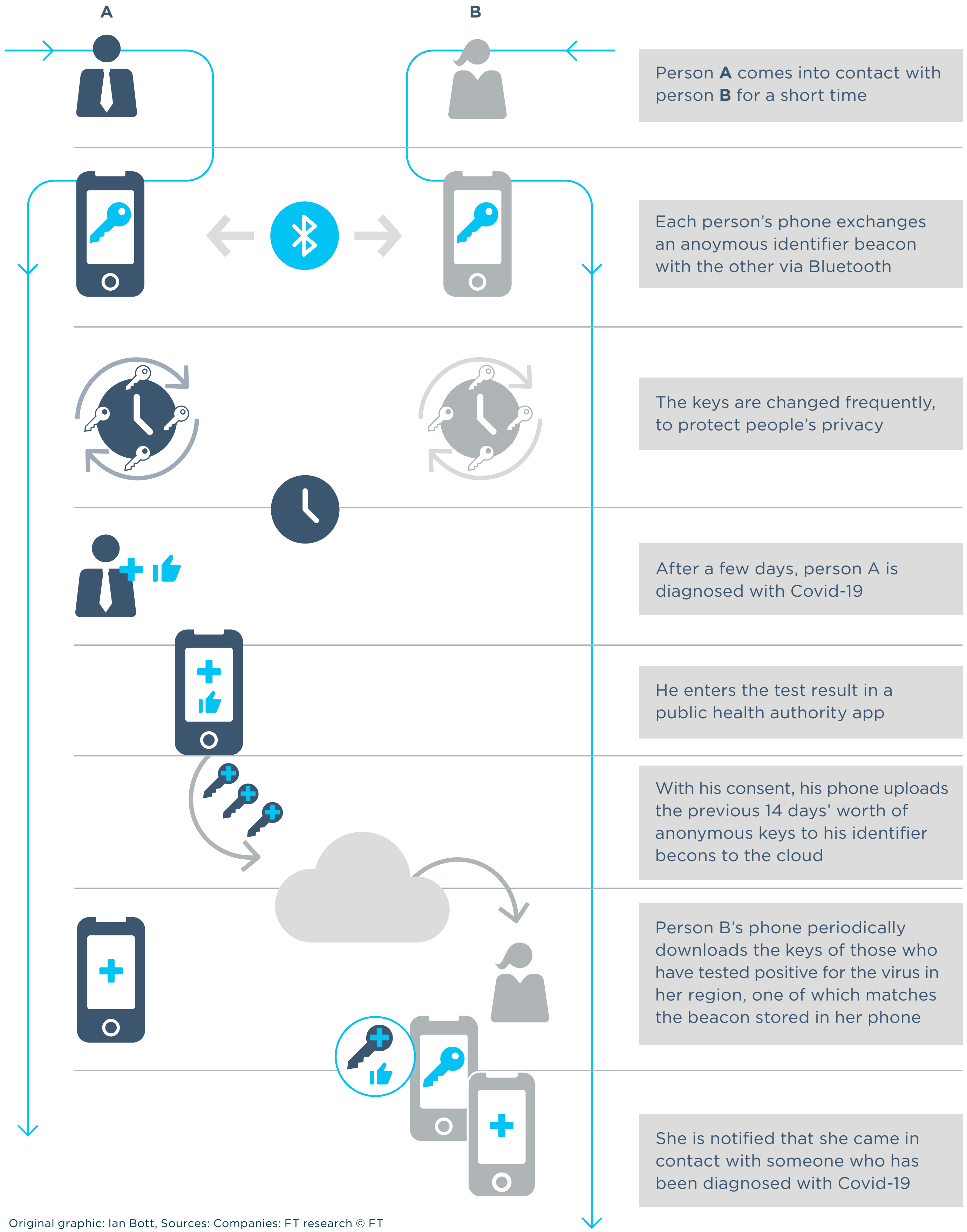
Indeed, in a unique collaboration move, Apple and Google have teamed up to join in the global effort against the pandemic by allowing their mobile operating systems to be used to operate the apps. By using Low Energy Bluetooth (i.e. Bluetooth that is always on), they are able to establish a decentralised contact-tracing framework (**CTF**), allowing connection to be made between phones which are in close proximity with each other. This is a major contribution as current apps using Bluetooth and smartphones do not allow the wireless protocol to operate constantly. The system will collate data from both Android and iPhone users who sign up to the app and is expected to be made available by mid-May 2020. It is also worth noting that both tech giants have been heavily investing in in the trillion-dollar health care industry in the past year but nothing may give them a bigger headway into the industry than this joint contribution to tracking the spread of coronavirus.

The main differentiator between the above discussed models resides in the storage location of troves of health and location data which comes with significant intrinsic privacy consequences:

- **Under the decentralised model**, such data would be kept on the users' devices. Users can opt-in to share their phone number or details of their symptoms, which would be used by health authorities to contact them and give advice on the best course of action in the event they are found to be at risk. This consent would be given in the app, instead of being part of the system's central architecture
- **Under the centralised model**, all data would be stored in a central server which may potentially open the door to government's mass surveillance in the absence of strong fundamental rights and security safeguards.

Showing the direction most EU countries are likely to take, Germany, where the shadow of historical institutionalised surveillance renders mass tracking very unpopular has now rallied to the decentralised model with an app deemed much less intrusive, relying on the Bluetooth "handshake" between two devices rather than tracking the location of individuals.

HOW CONTACT TRACING COULD WORK



Person **A** comes into contact with person **B** for a short time

Each person's phone exchanges an anoymous identifier beacon with the other via Bluetooth

The keys are changed frequently, to protect people's privacy

After a few days, person A is diagnosed with Covid-19

He enters the test result in a public health authority app

With his consent, his phone uploads the previous 14 days' worth of anonymous keys to his identifier becons to the cloud

Person B's phone periodically downloads the keys of those who have tested positive for the virus in her region, one of which matches the beacon stored in her phone

She is notified that she came in contact with someone who has been diagnosed with Covid-19

Original graphic: Ian Bott, Sources: Companies: FT research © FT

2. THE DATA PROTECTION LEGAL FRAMEWORK FOR THE EU APPS

A. THE EU LEGAL RESPONSE

As contact tracing and related technologies require the collection of a wealth of personal data from individuals ranging from basic identity information to device identifiers, location data and health information, the rules established by both the General Data Protection Regulation (EU) 2016/679 (**GDPR**) and the Directive 2002/58/EC (**ePrivacy Directive**) and UK's and EU member states' implementing legislation shall apply in the UK and the EU.

Taking the initiative for a coordinated approach across the EU, the European Commission (**EU Commission**) published on 8 April 2020 recommendations to develop a common EU toolbox for "the use of technology and data to combat and exit from the COVID-19 crisis" (**Commission Recommendations**). On April 15th, a toolbox was released by the EU's eHealth Network called "Mobile applications to support contact tracing in the EU's fight against COVID-19; Common EU Toolbox for Member States" (**EU Toolbox**).

Reportedly, the EU Commission is also closely scrutinising Google and Apple's collaboration to make their operating systems interoperable, in compliance with the EU Toolbox and privacy by design principles.

However, the call for a "pan-European and co-ordinated approach" may have come too late. It was only announced on 8 April 2020, in response to call from the European Data Protection Supervisor two days earlier. By then, many countries had already released apps or were well underway in preparing to launch.

Soon after the Commission Recommendations, the European Data Protection Board (**EDPB**) published two much-awaited guidelines on the 21 April 2020 which aim to provide practical guidance for GDPR-compliant Covid-19 contact-tracing apps.

In the first (Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (the Scientific Research Guidelines)), the EDPB reminds that the GDPR "foresees a specific derogation to the prohibition of processing of certain special categories of personal data, such as health data, where it is necessary for these purposes of scientific research" but that nevertheless "Fundamental Rights of the EU must be applied when processing health data for the purpose of scientific research connected to the COVID-19 pandemic."

> **“**
> **the voluntary basis of the app does not mean that consent is necessarily the legal basis for processing.**

In the second (Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the Covid-19 Outbreak (the Tracing Guidelines), the EDPB’s main takeaways focus on:

- **Location data:** The Directive 2002/58/EC (e-privacy Directive) applies to the processing of location data collected by electronic communication service providers and by information society service providers’ applications. Such data may only be transmitted to authorities or other third parties once anonymised or with prior consent of the user. Preference should always be given to processing of anonymised location data.

  The re-use of location data may be subject to additional conditions including additional consent or on the basis of EU or Member State Law such as national security, public security, or public interest.

- **Legal basis for the processing:** the voluntary basis of the app does not mean that consent is necessarily the legal basis for processing. The legal basis may be a GDPR compliant consent from the user but also public interest when the service is require by the EU or Member State’s law to which an individual is subject to.

- Apart from GDPR-compliant consent from the user, the necessity of performing a task in the public interest forms the relevant legal basis when public authorities provide a service required by EU or Member State’s law to which the controller is subject.

- **Data protection impact assessments (DPIAs)** must be carried out before implementing such apps and should be published.

- **General GDPR principles apply to the processing:**

  - To ensure accountability, the controller of any contact tracing application such the national health authorities should be clearly defined, and their roles and responsibilities explained to the users.

  - Explicit consent of the app user is required for processing health data except if EU or Member States law allows the processing if necessary for reasons of:

    - public interest in the area of public health such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices

    - i) preventive or occupational medicine, (ii) assessment of an employee’s working capacity, (iii) medical diagnosis, (iv) provision of health or social care or treatment of the management of health or social care systems and services, pursuant to contract with a health professional.

  - In compliance with the principle of data minimisation and the privacy by design and privacy by default principles, proximity data should be used rather than tracking location of individual users and collected information should reside on the user’s device.

  - Only relevant information should be collected from the user’s device and only when necessary.

  - Both centralised and decentralised approach may be acceptable but the decentralised solution is more in line with the minimisation principle

  - Appropriate measures should be put in place to prevent re-identification

  - The reporting of users as COVID-19 infected on the application must be subject to proper authorisation, for example through a single-use code tied to a pseudonymous identity of the infected person and linked to a test station or health care professional. If confirmation cannot be obtained securely, no data processing should take place presuming validity of the user’s status.

B. THE UK

The UK’s data protection regulator, the Information Commissioner’s Office (**ICO**), has given its approval to the above discussed decentralised CTF framework and the DP-3T in a statement on the Apple and Google joint initiative, dated 17 April 2020. This approval was given on the basis that these decentralised proposals “appear aligned with the principles of data protection by design and by default” and include restrictions to protect user privacy. The ICO was also satisfied that the CTF is designed to only generate a limited amount of data from the user’s device and concentrates its analysis on the data generated by cryptographic tokens (known as “identifiers”) created on that device, and stored tokens collected from nearby devices via Bluetooth. As tokens are not associated with other data that may further identify or locate the device user, it mitigates risks of re-identification.

However, the UK government, in tandem with the National Health Service (**NHS**), appears to have rejected Apple and Google’s plan in favour of a more centralised system that stores the matching information on a computer server which is deemed to offer the highest level of security. Although, it should be noted that health agencies involved in tracing are not immune to data breaches and would require to put in place adequate safeguards.

The NHSX UK app, which is expected to launch in May 2020, is still under development by NHSX, a Government unit set up early in 2019 with responsibility for setting national policy and developing best practice for NHS) technology, digital and data, including data sharing and transparency. NHSX has largely been developing the app in total confidentiality which has led to mounting concerns over lack of transparency, function creep and misuse of data instigating potential new forms of surveillance.

Despite these concerns, the ICO has released a statement, on 24 April, to confirm that it has been involved in the development of the NHSX tracing app and is helping NHSX to *“ensure a high level of transparency and governance”*. The statement goes on to clarify that the ICO will remain involved in the development and roll-out of the app. This involvement is at least an encouraging sign that the app is being designed in compliance with the GDPR principles and the provisions of the UK’s implementing legislation, the Data Protection Act 2018 (**DPA**).

NHSX has also disclosed on its website that it is collaborating with the ICO, the National Data Guardian’s Panel and the Centre for Data Ethics and Innovation. This collaboration is clearly an attempt to reassure the public of the robust security and privacy standards applied in the development of the app. Further reassurance can be found in the knowledge that future new releases of the app will enable people to *“choose to provide the NHS with extra information about themselves to help identify hotspots and trend”* and that *“the data will only ever be used for NHS care, management, evaluation and research.”* Evidently, NHSX aims to win public’s trust by vowing to apply, at all times, transparent standards of privacy, security and ethics in the creation of the app.

“

the legal bases for processing personal data contemplated by the app mainly rely on the explicit consent of the user.

LEGAL BASIS FOR THE PROCESSING OF THE UK APP:

Under the DPA and GDPR, the legal bases for processing personal data contemplated by the app mainly rely on the explicit consent of the user, public interest in the area of health, or where the processing is necessary and proportionate under the law of a member state law. These are discussed briefly below, and it should be noted they will broadly apply to the use of the different apps across Europe.

- **Consent:** this is a legitimate ground for processing under the GDPR, however, reliance on consent alone is not recommended: it can be withdrawn as freely as it has been given. Further, as has been recently clarified by the EDPB there is a distinction between overcoming privacy hurdles on the one hand (through the voluntary downloading and use of an app by the public) and the subsequent processing of the data by governments.

- **Necessity:** there are a number of different circumstances in which the processing of data may be necessary. As special category health data, the data generated by a contact tracing app will also require to satisfy certain additional conditions. In the context of Coronavirus, the most discussed condition is to *“allow the performance of a task carried out in the public interest”* on the basis that the processing is necessary to protect the public health. In the UK, there is an additional hurdle to meet under the DPA: the processing must be done as a function of government or by a person who has a duty to do so under an enactment or rule of law. Therefore, as a public body, the NHSX’s central role in the development of the UK apps is crucial.

- **Proportionality:** this data protection principle restricts authorities in the exercise of their powers by requiring them to strike a balance between the means used and the intended aim. In the context of fundamental rights, such as the right to the protection of personal data, proportionality is key for any limitation on these rights. In general, proportionate processing will usually be transparent, temporary and anonymous. The extent to which the UK’s centralised approach will satisfy these grounds remains to be seen and further ICO guidance on why it considers it to be compliant is eagerly awaited.

- **Privacy by design:** under this principle, security and privacy are to be prioritised at all stages of the app’s development, starting with the initial design and user testing.

- **Transparency:** this is another key principle of data protection law under which data subjects have the right to know which of their personal data are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

Publically, NHSX is committed to transparency in relation to the new app and undertakes to *“publish the key security and privacy designs alongside the source code so privacy experts can “look under the bonnet” and help ensure the security is absolutely world class”*. In order to ensure that the app complies with the highest technical standard and proves effective in the fight against COVID-19, an independent assurance board has also been established, which includes experts in mobile apps, data governance and clinical safety.

At the time of writing, the NHSX has clarified that *“Users of the app will remain anonymous up to the point where they volunteer their own details, and there will be no database that allows the de-anonymisation of users.”* It has also been confirmed a data protection impact assessment will be published in due course, and that the app will be closed once the threat from the pandemic has passed, with any data that users have chosen to share being deleted at that point, with only some retained for research purposes, subject to legal and ethical considerations, to *“better understand the virus.”*

C. FRANCE

A proponent of the centralised model, the French government has chosen to develop an application called “StopCovid” which will be made available on an anonymous and voluntary basis using Bluetooth technology and not location data.

On April 24, 2020, the French data protection authority (**CNIL**) published its opinion on “StopCovid”, and gave its approval in principle to the application on the basis that it would be developed in compliance with the concept of data protection by design and *“since it uses pseudonyms and will not allow lists of contaminated persons to be retrieved”*.

As the app will effectively process personal data, all processing will be subject to the GDPR and the CNIL recommends a number safeguards are put in place, as follows:

- In accordance with the purpose limitation principle, the app may only be used to alert people who may have come in proximity to the virus and for no other purposes like monitoring the compliance of confinement measures.

- It emphasises the need for measures to avoid tracing pseudonymised data back to individuals.

- In line with the principles of data minimisation and storage limitation, the data must be kept for a limited period of time and for no longer that is needed.

- In accordance with the EDPB recommendations in the Tracing Guidelines, the CNIL It acknowledges as well the necessity to carry out a data protection impact assessment. The CNIL considers that the data controller of the app should be the French Health Ministry or any other health authority involved in the health crisis management.

- Finally, the CNIL considers that the legal basis for the use of a voluntary contact tracing app helping to manage the current Covid-19 crisis should be based on public interest when the processing is carried out by public authorities. The legal basis for the specific processing of health data by the “StopCovid” application should be public interest in the area of public health. The Government will be expected to consult the CNIL on the draft legislation regulating the implementation and use of the StopCovid app.

As the app is awaiting parliamentary adoption, the CNIL will publish new recommendations on the architecture and security of the application. The CNIL is conscious that for the app to achieve its maximum potential, it will need to gain public trust and widespread adoption.

On the 26 April 2020, the National Cybersecurity Agency of France (‘ANSSI’) revealed the launch of a StopCovid project team, including members of the National Institute for Research in Digital Science and Technology (‘Inria’), Capgemini, Orange S.A., the National Institute of Health and Medical Research (‘Inserm’), and Withings France S.A., who will collaborate to develop the StopCovid app. The ANSSI has vowed transparency and compliance with the principles of data protection and the right to private life as defined under French law and the GDPR.

Furthermore, the ANSSI published its recommendations on 27 April 2020 to Inria regarding the digital security and information security of the StopCovid app. In particular, it refers to security measures such as the use of a digital safe to protect the central server and transmitted pseudonymised information, the use of Bluetooth technology, and the encryption of pseudonyms with the SKINNY-64/192 algorithm.

As in other EU countries, French MPs and civil liberties groups have voiced concerns of the risks of state surveillance and privacy in the design and management of the StopCovid app. Further shadows loom on the app which is set to launch on the 11 May as it will not be able to deploy all functionalities on iPhones. Apple would need to change its current iOS settings and policies that include Bluetooth restrictions not permitting the transfer of data collected by Bluetooth apps from a device to centralised servers.

D. GERMANY

Until recently, the German government was a strong advocate of the centralised PEPP-PT initiative which is currently supported by the European health agencies, in particular the NHS in the UK and those in France. However, from the 26 April 2020, Germany has decided to back a decentralized system. This change of tack is clearly motivated by growing privacy concerns in relation to the centralised data model.

Much like the ICO and the CNIL, the German data protection commissioner (*Datenschutzkonferenz*) fully supported the recommendations of the EDPB for a GDPR compliant contact tracing technology, urging for health authorities and developers to design and implement such tools in a transparent manner and on a voluntary basis. According to the Datenschutzkonferenz, an individual tracking or a later re-personalization functionality should be excluded.

Germany has decided to introduce contact tracing tools based on the API of Google and Apple, a decision prompted by the need to ensure a quicker launch of the app. Further, as in the UK and in France, the app will be made available on a voluntary basis, meet German and EU data protection standards and guarantee a high level of data security.

The “Datenschutzkonferenz” has highlighted in its “Resolution on data protection principles” published on the 3 April 2020 that the processing of personal data must be justified under the appropriate legal basis during the COVID-19 crisis. It calls for the evaluation and implementation of appropriate, proportional and effective measures. The “Datenschutzkonferenz” expresses concerns over the use of location data to track individual infection patterns and does not recommend its use. It recommends for any data processing required for contact tracing purposes to be reversible and time-limited so as to apply only as long as necessary. The app will also need to comply with the highest possible cyber security standards.

Much like the other apps developed in the EU, the app will exchange temporary encrypted identity data and will notify the individual who has been in close proximity to an infected individual without revealing the identity of such individual, but also ensuring there are adequate rules in place to protect people who are being asked to trust both technology companies and the government with their data, freedom and well-being.

> **“**
> **Germany has decided to introduce contact tracing tools based on the API of Google and Apple, a decision prompted by the need to ensure a quicker launch of the app.**

3. CONCLUSION AND TABLE

In conclusion, the success of European contact tracing apps will depend on the widespread adoption by the population in each jurisdiction and the ability of governments and health authorities to win the trust of the public. To earn public support, transparent communications to the public will be required as well a very strong focus on the security and privacy of the users.

The different technical models adopted by the European countries raise concerns about the cross-border interoperability between the contact tracing apps once the borders reopen. Fundamentally, the adoption of contact tracing apps to help getting through the Covid-19 health crisis gripping every single country in the world will put to test the balance between state surveillance and user privacy.

THE TABLE BELOW HAS BEEN COMPILED AS A REFERENCE POINT FOR THE MAIN EUROPEAN PRIVACY-CENTRIC INITIATIVES AND RECOMMENDATIONS PUBLISHED TO DATE.

INITIATIVE / RECOMMENDATION	SUMMARY	CENTRALISED / DECENTRALISED	BLUETOOTH?	STATUS AND LINK
Decentralised Privacy-Preserving Proximity Tracing (**DP-3T**)	Open protocol for proximity tracing using Bluetooth functionality on mobile devices that ensures personal data and computation stays entirely on an individual's phone. It was produced by a core team of over 25 scientists and academic researchers from across Europe.	Decentralised	Bluetooth	Various versions published, being updated on a rolling basis. **https://github.com/DP-3T/documents**
Pan-European Privacy-Preserving Proximity Tracing (**PEPP-PT**)	A software system created to assist national initiatives by supplying ready-to-use, well-tested, and properly assessed mechanisms and standards. Currently a 'closed' initiative, with little by way of published details of how the software works. Criticised by DP-3T for lack of transparency. Reportedly feeding into apps for France, Italy and Germany, among others	Centralised	Bluetooth	Software in development, with contributions encouraged. **https://www.pepp-pt.org/**
European Data Protection Supervisor (**EDPS**)	Statement calling for a pan-European approach to development of contact tracing apps.	N/A	N/A	Published 6 April 2020 **https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf**
European Commission Toolbox and Guidance	EU guidance for the use of mobile apps for contact tracing in response to the coronavirus pandemic. Part of a common coordinated approach to support the gradual lifting of confinement measures. It includes: - recommendations to develop a common EU toolbox for "the use of technology and data to combat and exit from the COVID-19 crisis" (the "Recommendations") - a toolbox, released by the EU's eHealth Network called "Mobile applications to support contact tracing in the EU's fight against COVID-19; Common EU Toolbox for Member States" (the "Toolbox").	Recommends decentralised models	Recommends Bluetooth models	Published 6 and 8 April 2020 **https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670** Published on 6 April 2020 **https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf** Published on 8 April 2020 **https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf**
European Data Protection Board (**EDPB**)	Open letter setting out EDPB's views on the development of legally compliant apps and the need for a co-ordinated European approach Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the Covid-19 Outbreak (the Scientific Research Guidelines).	Recommends decentralised models	Recommends Bluetooth models	Published 14 April 2020 **https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf** Published on 21 April 2020 **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf** Published on 21 April 2020 **https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf**
UK Information Commissioner (**ICO**) NHSX	Opinion on Apple and Google joint initiative on COVID-19 contact tracing technology Blog: Digital contact tracing: protecting the NHS and saving lives	Centralised	Bluetooth	Published on 17 April 2020 **https://ico.org.ukmedia/about-the-ico/documents/2617653/apple-google-api-opinion-final-april-2020.pdf** Published on 24 April 2020 **https://www.nhsx.nhs.uk/blogs/digital-contact-tracing-protecting-nhs-and-saving-lives/_**
The French Data Protection Authority (**CNIL**)	Coronavirus (Covid-19): reminders from the CNIL on the collection of personal data Opinion on the development of the 'StopCovid' contact tracing app	Centralised	Bluetooth	Published on 6 March 2020 **https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles** Published on 26 April 2020 **https://www.cnil.fr/sites/default/files/atoms/files/deliberation_du_24_avril_2020_portant_avis_sur_un_projet_dapplication_mobile_stopcovid.pdf**
Germany Datenschutzkonferenz	Resolution on data protection principles	Decentralised	Bluetooth	Published on 3 April 2020 **https://www.datenschutzzentrum.de/uploads/dsk/20200403-DSK-Entschliessung_Pandemie.pdf**

GET IN TOUCH

DR. NATHALIE MORENO

Partner

+44 (0)20 7160 3179
+44 (0)7921985931
nathalie.moreno@addleshawgoddard.com

PROBLEMS. POSSIBILITIES.
COMPLEXITY. CLARITY.
OBSTACLES. OPPORTUNITIES.
THE DIFFERENCE IS IMAGINATION.
THE DIFFERENCE IS AG.

addleshawgoddard.com

This document is for general information only. It is not legal advice and should not be acted or relied on as being so, accordingly Addleshaw Goddard disclaims any responsibility. It does not create a solicitor-client relationship between Addleshaw Goddard and any other person. Legal advice should be taken before applying any information in this document to any facts and circumstances. Addleshaw Goddard is an international legal practice carried on by Addleshaw Goddard LLP (a limited liability partnership registered in England & Wales and authorised and regulated by the Solicitors Regulation Authority and the Law Society of Scotland) and its affiliated undertakings. Addleshaw Goddard operates in the Dubai International Financial Centre through Addleshaw Goddard (Middle East) LLP (registered with and regulated by the DFSA), in the Qatar Financial Centre through Addleshaw Goddard (GCC) LLP (licensed by the QFCA), in Oman through Addleshaw Goddard (Middle East) LLP in association with Nasser Al Habsi & Saif Al Mamari Law Firm (licensed by the Oman Ministry of Justice), in Hamburg through Addleshaw Goddard (Germany) LLP (a limited liability partnership registered in England & Wales) and in Hong Kong through Addleshaw Goddard (Hong Kong) LLP, a Hong Kong limited liability partnership pursuant to the Legal Practitioners Ordinance and regulated by the Law Society of Hong Kong. In Tokyo, legal services are offered through Addleshaw Goddard's formal alliance with Hashidate Law Office. A list of members/principals for each firm will be provided upon request. The term partner refers to any individual who is a member of any Addleshaw Goddard entity or association or an employee or consultant with equivalent standing and qualifications.