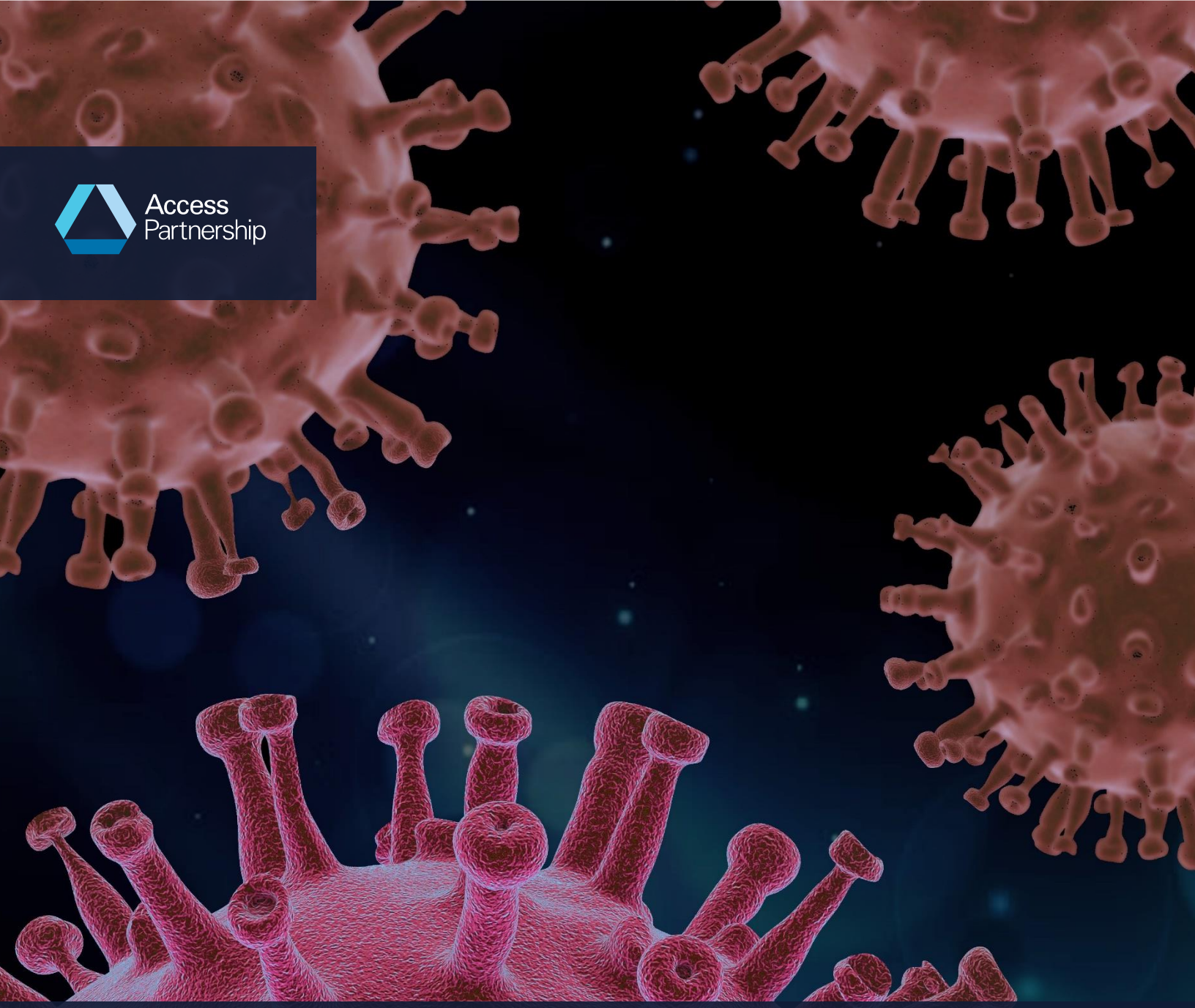


Access Partnership

Digital Contact Tracing

A Comparative Global Study

Access Partnership 2020

Contents

Foreword

What is written can be unwritten, what is downloaded can be deleted, and so the digital tracing of contacts between people who risk infection by a punishing virus is broadly to be welcomed. That contact tracing also heightens anxiety about citizen privacy can also be celebrated, at least for the validity of the concern if not for the negative effect it has on uptake of this important tool. This study shows what approaches are best at building citizen confidence.

Scope

Undertaken to provide a timely overview of how *tech-enabled* countries have approached use of digital contact tracing to stalk and defeat COVID-19, the insights that follow can be used to predict how the virus crisis will affect privacy policy worldwide. Our findings reveal that, regional variations notwithstanding, privacy is taking a back seat to health concerns across the board.

Methodology

Our researchers used up-to-the-minute data on national approaches which was validated where necessary by engagements with national stakeholders and policymakers. Questions to officials were informed by the team's use of Access Partnership's proprietary database of privacy laws, regulations, and qualitative assessments of how these are applied in each jurisdiction. The timeframe for production of this study was a narrow ten working days.

Understanding the Gaps

While this report explains the extent to which national approaches to contact tracing vary, a majority of countries have no such option at all. The requisite digital tools for effective contact tracing – access to smartphones, operating systems and platforms, Bluetooth equipment, apps, and wireless communications – are not available to all countries in equal measure. In that 49% of the world which remains digitally unconnected, virus fightback must start with adoption of policies that enable countries to take advantage of great leaps in pandemic-busting ingenuity. In this, as in matters of coding, cloud and connectivity, technology firms worldwide are ready with technical solutions and policy advice to governments. *Their* offers of help should not be ignored: made in good faith, they seek to be equitably distributed, and foresee a shared legacy that can outlast both this virus and the equally tricky technology gaps that stand in the way of its defeat.

Gregory Francis
Managing Director

Executive Summary and Recommendations

Until recently, contact tracing was conducted manually on patients by doctors, nurses, and public health officials, and mostly over the phone: a patient's steps were retraced to locate the source of infection and alert sent to others that may have come into recent and close contact with the patient. This work had to be conducted by medical professionals who had an understanding of how diseases spread and "detective-like" skills.

The COVID-19 pandemic has spurred a rise in the use of digital tools in contact tracing. While armies of professional contact tracers are still being deployed globally, their work is supplemented by new ways of tracking and communication. Digital technologies, especially mobile technologies, have given rise to new sources of data that governments around the world are seeking to harness, the better to track those who may be infected, and they are transforming this traditional practice.

Governments are still in the early stages of building these systems, typically based on either geolocation history of individuals or records of recent contacts gathered wirelessly view Bluetooth, often leveraging mobile apps. The nascent stage of these efforts and the mix of national experiences means it is too early to render a conclusive judgement on the efficacy of these measures. But, as the national snapshots described below show us, they are nonetheless likely to have significant impacts on digital policy and the politics that surround it in many countries.

Still in the early days of digital contact tracing, countries are experiencing many challenges. Several national debates feature controversies over expansionary government surveillance: how much of it is required to ensure public health? Will it be permanent? Legal authorities everywhere are rushing to articulate or decide how the processing of personal health data in emergencies is or should be grounded in law. Governments and companies with global reach are at odds over who should hold the power – legally and practically – to determine the treatment accorded to personal information in a national emergency.

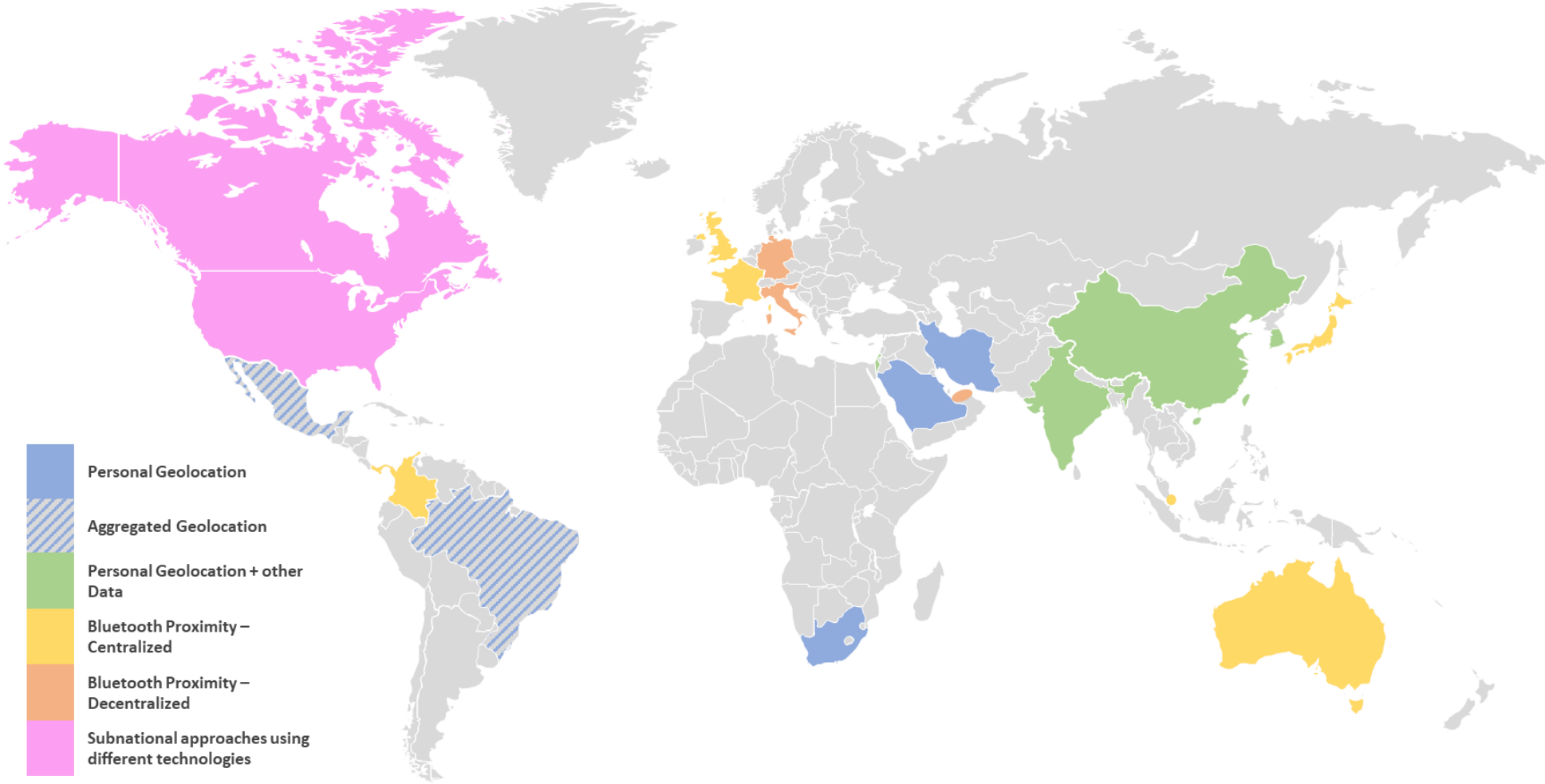
These questions are at the core of deep challenges for digital policy in the twenty-first century. They must be resolved through inclusive national, as well as global dialogues. Though policymakers can and will weigh these questions differently, we recommend several guiding principles to ensure the continued expansion of digital technology on terms that are fair and beneficial, globally:

- **Close public-private cooperation and dialogue** – Both governments and companies hold critical and legitimate roles in jointly building effective and equitable responses. While governments rightfully claim extraordinary powers to protect public health, many digital contact tracing methods would be impossible without the technology provided by the private sector. While it is incumbent on the private sector to be responsive to governments, they also have a stake in safeguarding trust in use of their technologies and defending user's rights, while offering capabilities equitably around the world. Close dialogue and mutual accommodation are necessary to strike this balance.

- **Maximum interoperability** – Governments everywhere face similar problems. While experimentation in responses is healthy and will help the world arrive at best practices, persistently fragmented responses will undermine effectiveness and universal access to the benefits of digital contact tracing. Governments should seek to participate in common efforts and avoid fragmentation at the technical and policy levels that will impair cooperation now and in the future.
- **Safeguard the public trust** – Trust in digital technologies underpins not just the continued expansion of the digital economy and its benefits, but also the very efficacy of digital contact tracing efforts now. Many of these rely on individual consent and voluntary participation. As a result, transparency, clear communication, and credible steps to allay public concerns are indispensable.
- **Prepare for the next crisis** - Work must be done hastily to respond to emergent situations for which most the world was unprepared. However, the countries that have responded most effectively have been those with policies and systems already in place to facilitate responses. As governments take emergency measures, they should look to global best practices and lay the legal framework, policy structures, stakeholder connections, and technical capabilities to grapple with future crises. Constructing these mechanisms in advance will lead to both more effective responses and better privacy protection.

Date of Information: 22 May 2020

National Approaches to Digital Contact Tracing



Typology of Digital Contact Tracing

Contact tracing – or the systematic reconstruction of historical interactions of an infected person – has long been a standard tool of epidemiology and public health. Analogue modes of information gathering, such as interviews, conducted by teams of hundreds or thousands of trained workers, have been and continue to be widely deployed to combat disease outbreaks. Digital technologies have given public health officials the opportunity to transform traditional modes of doing contact tracing. Increasingly pervasive personal uses of technology—especially smartphones—and digitalisation of everyday transactions, such as in retail and transportation have resulted in a huge quantity of data that could be used to track and reconstruct how an individual with a disease has interacted with others.

These approaches are being deployed now in many different countries. However, due to the various types of data available, different legal frameworks, and divergent political values, there are different ways that governments have constructed systems for digital contact tracing.

	Geolocation	Geolocation Plus	Proximity Tracing (centralised)	Proximity Tracing (decentralised)
Technology used?	GPS, mobile phones	GPS, mobile phones **and** other digital technologies, including digital payments cards, CCTV, etc	Smartphones, Bluetooth Low Energy, OS and apps	Smartphones, Bluetooth Low Energy, OS and apps
Cooperating industry stakeholders?	Mobile carriers	Mobile carriers, software and app developers, merchants, infrastructure operators, etc.	Software and app developers	Software and app developers
What information is collected/processed?	Absolute location	Absolute location **and** others including payments, biometrics, etc.	Identifiers of others in close proximity, personal identifiers	Identifiers of others in close proximity
Voluntary/consent-based?	Typically, no	Typically, no	Yes	Yes
Is data personally identifiable?	Yes	Yes	No/Maybe (anonymous or pseudonymous)	No (anonymous)
Who can personally identify contacts?	Government	Government	Government or other system administrator (under some conditions)	No one
Who decides when to notify individuals?	Government	Government	Government OR diagnosed individual	Diagnosed individual

Geolocation

One of the simplest ways in which governments are using digital technology to track potentially infected individuals is with location data. Using GPS, mobile phones can register the geographic location of the device with a reasonable degree of accuracy. By accessing this data and analysing large time series datasets, governments are able to reconstruct the movements of someone later diagnosed with COVID-19 and the individuals they have previously come into close proximity with. However, there can be accuracy challenges with GPS data. Specifically in built up areas, locations registered on devices can experience errors of 10 meters or more.[1] While accurate enough to raise privacy concerns, these data sets may not always provide reasonable certainty of proximity within a range that could be epidemiologically hazardous. Additionally, because of the uses of this approach for law enforcement and surveillance, this is one of the more controversial applications of digital contact tracing. Utilisation of this method involves personally identifying individuals and their movements to a high degree of specificity with highly sensitive implications. Without personally identifying contacts, several governments are also using geolocation data sets in an aggregated and anonymized format to understand macro trends and analyse community spread without specifically tracing contacts.

Geolocation Plus

Given the profusion of personal data that most individuals in developed digital economies generate daily, there are many other digital traces available to reconstruct past contacts. Some governments are increasingly turning to them in order to supplement geolocation data. These may include records generated by digital payments that can identify precisely when and where an individual visited a place of business, or public surveillance such as CCTV footage, in some cases enabled with facial recognition technology. In several instances, government applications which are primarily based on Bluetooth proximity tracing – discussed below – may utilize GPS data to pinpoint individuals' locations more precisely, ameliorating accuracy challenges that can result from either GPS or Bluetooth alone to determine proximity.

Zoom-In: Apple & Google

On 10 April, Apple and Google announced [2] an unprecedented collaboration to enable a system for contact tracing apps that work across both of their two platforms. The two smartphone OS developers are jointly creating a set of APIs to enable a public health authority to construct contact tracing apps on the basis of Bluetooth Low-Energy (BLE) proximity tracing.

Phones operating the app will continuously broadcast rotating anonymous identifiers associated with the individual, which other phones within a certain distance will register and store for a period of two weeks. If an individual is later diagnosed with COVID-19 and consents to upload their data, other phones are alerted of that person's identifiers and will check against those it is storing. If there is a match, the app will notify the user that they have been in close contact with an infected person.

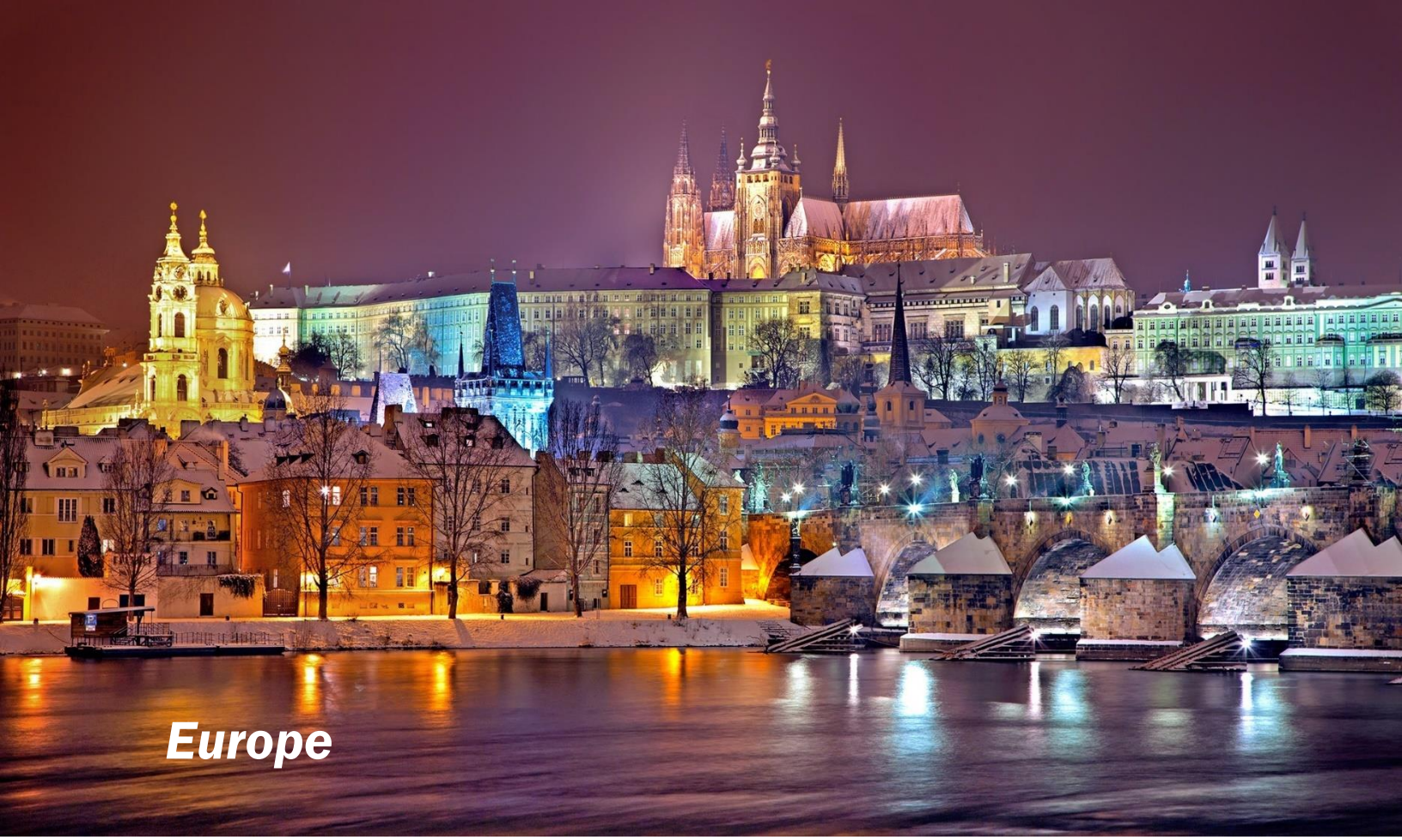
At a technical level, this collaboration among competitors is indispensable to enabling systems based on BLE proximity tracing. In addition to enabling software changes that maximize the effectiveness of the BLE approach, it means that smartphones from the world's two dominant mobile operating systems would be able to operate the same app and communicate seamlessly.

Bluetooth Proximity Tracing

Perhaps the most widespread approach to digital contact tracing relies on use of Bluetooth Low-Energy (BLE) capabilities built into nearly every smartphone. By emitting a short burst of connectivity and measuring the power received from other devices, smartphones can estimate the physical distance separating one from another. In digital contact tracing, this technology can be used for devices to swap anonymous identifiers. When an individual later tests positive for COVID-19, devices containing the identifiers associated with that person can notify them of the need to self-isolate or seek medical attention. The privacy advantages of this approach are clear since identifiers are anonymous. Device users—and depending on the implementation even public health authorities—would be unable to know the specific contacts a person has had.

There are limitations to this approach. Smartphone ownership, as well as digital contact tracing enablement are both affirmative opt-in decisions. Smartphone penetration averages just 76% across advanced economies and can be far lower in developing economies, limiting the ability to gather data from a critical mass of the population necessary to blunt the virus's spread.[3] Since a system using BLE relies on measuring apparent signal strength, it may not provide reliable indications of distance and may be confused by the presence of physical obstacles, making a signal appear closer or further away than it is. Additionally, it may ignore barriers which may prevent the spread of the virus but not Bluetooth signals such as a wall or window. Furthermore, smartphone operating systems typically restrict the ability of applications to utilise Bluetooth unless directly in use. As a result, a phone may not be able to broadcast or receive an identifier unless the phone is unlocked and/or the application is in active use.

Regional Trends



Europe

As one of the global epicentres of the COVID-19 crisis, European public health authorities are rushing to construct systems for digital contact tracing. However, fragmented and overlapping political authorities and public urgency are resulting in various European countries moving at different speeds and in different directions, experimenting with approaches to build both effective systems and public trust.

The European Union, eager to remain relevant in a crisis that has seen muscular exertion of its members' nation-state powers, has in some respects played catch-up. While pressing for the continued application of General Data Protection Regulation (GDPR) and trying to position itself as a world leader in privacy-protecting approaches, Europe has struggled to facilitate and coordinate interoperable approaches to digital proximity tracing at a continental level.

European Union

The European Union's greatest challenge is how to coordinate a joint approach to contact tracing among its 27 member states when members have divergent views on the level of privacy that contact tracing systems need to ensure. The European Commission has taken the view that technology such as contact tracing apps can be developed and implemented within the GDPR, despite initial criticism that the privacy regulation would make it difficult or even impossible to develop and deploy high-tech responses to the COVID-19 crisis. The Commission published guidance on 17 April, along with a toolbox for member states on

the use of mobile applications for contact tracing.[7] The guidance affirms that GDPR and the ePrivacy Directive provide the strongest safeguards of trustworthiness, namely enshrining a voluntary approach, data minimisation and time limitation.

The European Data Protection Board (EDPB, the group of national data protection regulators), which adopted its own guidelines on 21 April, is of the same view regarding specific rules for the use of anonymous or personal data.[8] In its guidelines, the EDPB emphasised the need for such applications to remain voluntary, to rely on proximity information regarding users rather than on tracing individual movements and calls for careful processing and "robust anonymisation techniques."

Fundamental rights are here to stay?

The EU has built in time-bound actions to review the effectiveness of the apps at national, cross-border and Brussels level. It remains to be seen, however, to what extent member states will choose to follow these rules, with countries such as Hungary already being admonished for "democratic backsliding" following the adoption of a text which allows the government to implement extraordinary measures by decree for a virtually unlimited period of time.[9]

Zoom-in: PEPP-PT

The EU developed the PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) project, [4] a consortium of eight countries and over 100 experts working to assist national initiatives by supplying ready-to-use mechanisms and standards. The aim of the group was to ensure European citizens would not have to abandon what they understand as fundamental privacy rights. The idea was to enable a solution which could be accepted across the EU while at the same time enabling an effective tool for proximity tracing that would make a real difference in the fight against COVID-19.

Less than a month after its creation, reports of splits within the group and criticism over a lack of transparency started to emerge.[5] Several researchers and academic institutes from Switzerland, Germany, Italy and Belgium chose to leave the PEPP-PT initiative over questions about transparency and data privacy. The main split in opinion has been on whether the "decentralised" app designs are better at preserving privacy than "centralised" models. The future role of the project is uncertain, with member states moving[6] to other industry-led solutions, at a time when contact tracing solutions are urgently needed as EU countries begin embarking on their COVID-19 exit strategies.

United Kingdom

The UK, after initially dismissing South Korea's strategy on contact tracing, has experienced a 'Road to Damascus moment' on the test, track and trace approach. The UK faces challenges in all three prongs. First, in having to ramp up testing capacity to 100 000/day in a few weeks and then to 250 000; second, in the appropriate size of the contact-tracing 'army' (current target: 18 000, although some experts say it must go higher); now too, in the third, Britain is hitting roadblocks.

Unlike in other jurisdictions, this is not because of public resistance. High public trust of the NHS, the app's developer, lowers the risk of it being caught up in partisan divisions. Early polling suggests high levels of support for using smartphones to fight the pandemic – 65% support or strongly support smartphone-powered contact tracing, while 49% would even

support using phone tracking to police individual behaviour.[10] Tech trials began on 4 May on the Isle of Wight and saw a rapid adoption rate of around 50% and counting (at time of writing).

The UK is trying to swim against the tide set by Apple and Google in its tracking app design. Like other apps in this report, NHS CV-19 relies on BLE, and keeps an anonymous log of devices it has been within close proximity to and alert affected individuals if someone in the chain is diagnosed with COVID-19. Unlike other countries and in contrast to the functionality offered by Google and Apple, data will be pooled and monitored centrally. This means it will not operate in the background, potentially requiring a swift technical redesign which the NHS' technology lead, Matthew Gould, said was sapping credibility. UK Health Secretary, Matt Hancock, has said the app's use would be voluntary, and reassured people that its data would be for limited uses and deleted once the emergency was over.

Compounding these difficulties, the government is facing criticism from privacy campaigners on an internal policy memorandum that suggested data could be 'de-anonymised' at a later point, which could undermine trust and adoption. More importantly, this could run afoul of GDPR in the UK, which, at least until January, remains enforceable at the European Court of Justice and against which the UK must be considered adequate by the European Commission to continue personal data flows with Europe uninterrupted post-Brexit. Meanwhile, the government faces an increasingly restive parliament and has competition in devolved administrations in Scotland, Wales, and Northern Ireland for leadership.

Germany

Widely seen as one of Europe's more successful states in the fight against COVID-19, Germany has been central to the debate about the role of location tracking and contact tracing apps since the debate kicked off. Unusually for a European country, Germany has a Federal Data Protection Authority—as opposed to unitary—and a separate authority for each state, creating an army of voices to intervene on the privacy considerations of any technology used in the COVID-19 response. Discussion of any kind of large-scale surveillance is a sensitive topic amongst Germany's privacy-conscious citizens and Lander.

The EU's PEPP-PT system (see above) traces its origins to Germany. However, the Federal Government has decisively changed tack, announcing on 27 April that it will move away from PEPP-PT and support a separate decentralised approach.[11] Reporting indicates that the government felt that Apple's refusal to alter iPhone settings meant that the centralised approach was doomed to failure and that the decentralised approach was more likely to win the trust of German citizens.[12] Trust is key precursor to adoption, with estimates that 50 million Germans will need to download a contact-tracing app for it to be successful.[13] In announcing the change of policy, Germany's Health Minister, Jens Spahn, noted that Europe's lack of a large-scale manufacturer of mobile devices or operating systems left Germany little option other than to rely on US firms.

Instead, Germany will partner with two of its industrial giants, SAP and Deutsche Telekom AG to develop a decentralised national app, along with other undisclosed partners, likely making use of the joint Apple/Google initiative. The government has indicated that use of the app, called "Corona-Warn-App", will be voluntary. The app is set for launch in early June. The government is also planning an update for

later in the year which will allow users to voluntarily share data with Germany's national disease control center for use in research. SAP and Deutsche Telekom have promised that the app and backend will be entirely open-source and have published documentation on GitHub.[14] The documentation notes that the app is heavily inspired by the DP-3T[15] (Decentralised Privacy-Preserving Proximity Tracing) and TCN[16] protocols and based on the Privacy-Preserving Contact Tracing specifications[17] by Apple and Google.

France

In early April, the French Health Minister Olivier Véran explained that the government was thinking about developing a mobile application to "limit the spread of the virus by identifying chains of transmission." The objective was to warn people who have been in contact with a patient who tested positive, so that they can themselves get tested or isolate. The application called "StopCOVID" is now under development and should be available by the end of May. The French Institute for Research in Computer Science and Automation (Inria) is leading a consortium of researchers, cybersecurity experts and companies like Orange, Capgemini, and Dassault Systems in the endeavour.

However, technical problems have slowed down their work including compatibility with iPhones. Instead of attempting to adapt the application, French authorities have requested Apple to *turn off some privacy and security features* to allow the iOS to allow being transmitted via BLE and publicly criticized the company for refusing to do so.[18] In an attempt to reassure users, the French Government has stated the data would only be stored locally, with the healthcare authority acting as the data controller. The app, installed voluntarily on people's smartphones, would not track their locations or movements, and would use only BLE technology to help trace a person's recent contacts. Cedric O, the Secretary of State in charge of digital, said that after studying the tracking technology used in Asia, France has settled on the least intrusive technology.

Some in France see it as a profound cultural shift. StopCOVID has already drawn fierce opposition, including within President Macron's party. "Monitoring infected people is a dangerous and reprehensible response. The collection of personal information from mobile users (…) amounts to placing the population on an electronic bracelet," denounced the LREM Deputy Sacha Houlié in an op-ed, warning against "simplistic solutions and quick responses."[19] His colleague Guillaume Chiche deplores "the way in which, during a period of fear, some seek to accept the shrinking of our rights." CNIL, the national data protection authority said the app would comply with French and DU privacy rules but called for "vigilance."

Those defending the app argue that StopCOVID will alleviate the severe restrictions imposed in France and allow for a restoration of the basic freedom to come and go, visit loved ones, and work.[20] One member of the French National Assembly, Eric Bothorel, fiercely supports this project saying "There is no data collection. It is not tracking; it is not data collection. It's not the American Wild West or the Chinese Big Brother."[21]

Prime Minister Edouard Phillipe, who initially refused to have a debate and a vote at the National Assembly, finally promised a debate and a vote on the StopCOVID app, scheduled for 25 May. The assembly debate will be held in parallel with the debate on a bill, the Health Emergency Law (*ou loi d'etat d'urgence sanitaire*), that will extend the state of emergency until 24 July.[22] The Bill, which sets the rules to ease emergency health measures, includes under Article 6 authorities for "implementation of an information system which may in particular include health and identification data for the purpose of determining the persons infected or likely to be infected," and is raising similar privacy and security concerns as StopCOVID app.

Zoom-in: Corporations or government—which present the bigger privacy threat?

The tensions between government and industry are best demonstrated by ROBERT: a Franco-German Bluetooth protocol at odds with the Apple/Google led vision.

ROBERT associates Bluetooth identifiers with permanent IDs in a centralised database run by the government, where individuals are assigned a risk score based on numbers of interactions and are notified accordingly. Apple and Google's approach, by contrast, notifies affected phones without centralised government processing.

However, for ROBERT to be fully effective, changes must be made to operating parameters and permissions to allow constant Bluetooth broadcasting. The companies have so far refused to enable this centralized approach on privacy grounds, putting these governments on a collision course with big tech—again.

The developers of ROBERT argue that their approach is more privacy-protective than the Apple/Google protocol since it does not involve broadcasting identifiers of infected individuals, who could in theory be reidentified.

The tension underlines competing understandings of the primary source of privacy risks in digital contact tracing: abuses by governments who know too much about you, versus abuses private (American) corporations.

Italy

Despite Italy being one of the first and worst hit European countries in the COVID-19 pandemic, and despite the creation of multiple committees and task-forces to handle national responses to the emergency, digital contact tracing solutions have not yet been made available on a pan-Italian basis.

In mid-April 2020, selection of an iOS and Android app called *Immuni,* developed by Milanese tech company Bending Spoons, was recommended by the Minister of Innovation Paola Pisano, ostensibly based on an assessment conducted by a 74-expert strong "Data-driven anti-COVID Task Force". Later it emerged that the Task force in fact recommended to run parallel trials of two separate apps to seek some level of redundancy in case one of the solutions was not effective, and that the Minister unilaterally decided to limit the choice to *Immuni*.

Nonetheless, the National Technical-Scientific Committee coordinating the emergency response, adopted the Ministry's recommendation issuing an ordinance establishing contractual arrangements for the contact-tracing system. Privacy Guarantor Antonello Soro, in an opinion of 29 April 2020, acknowledged compliance of the system with European Regulations and with guidelines issued by the European Data Protection Board.[23] It clarified that the use of the app, as well as any processing of personal data must end at the termination of the state of emergency, and in any case no later than 31 December 2020. Finally, on 30 April, with the publication of Decree Law 28, the Italian government outlined the legal framework for the use of the contact-tracing app in the country.

Immuni's developers, in agreement with the Ministry of Innovation, decided to change the approach to the app's development, initially based on the PEPP-PT model. To increase privacy and data security, the app is now being designed to align to Apple-Google standards, pursuing decentralised Privacy-Preserving Proximity Tracing (DP-3T) approach. The Ministry for Technological Innovation and Digitization also committed to make the application's code open source and therefore usable by other governments in the fight against the virus.[24]

Aside from the Minister of Innovation's misrepresentation of the app selection process, criticism of the implementation of contact-tracing solutions were fuelled by government statements that the app could be effective even if only 25-30% of the population uses it, contradicting an initial estimate that 60% is the minimum threshold for effective utility. Since the Italian Constitution places healthcare under the remit of the federated Italian regions, rather than the central government, some local authorities have launched alternative solutions at the risk of impairing a coordinated response. The Head of the Italian national task force for COVID-19 response Phase II and ex-Vodafone CEO Vittorio Colao commented that it is critical to launch the app by the end of May and ensuring that it will be available for all citizens in the summer; otherwise it will serve little purpose.

Asia

Asian governments have taken a diversity of approaches befitting the diversity of cultures, political systems, and experiences of the pandemic to date. While some like China and South Korea have taken broad and aggressive approaches that rely on gathering, analysing, and sharing vast amounts of personal data, others have taken a more limited approach based on BLE. Overall, officials and publics seem to be more comfortable than Europeans making the bargain that they must sacrifice some privacy to fight the spread of the virus and governments tend to centrally manage digital contact tracing data.

China

China, ground-zero of the COVID-19 outbreak, utilized technology to assist with contact tracing by partnering with media giants Alibaba and Tencent. On 11 February, the Alipay "Health Code" was launched in Hangzhou, through the Alipay app.[25] The project was a collaborative effort by local government officials and Alibaba. The app assigned colour codes — red, orange, or green — to users, requiring those with red or orange codes to self-isolate for 14 or 7 days, respectively. Those assigned with the green code are required to show proof and scan QR codes when entering malls, restaurants, buses, schools, and other public places to declare they are healthy and record their movement. Colour codes are believed to be assigned based on self-reporting, government data (such as information relating to the movement of confirmed COVID-19 patients), and situational risk factors.[26]

On 15 February, the Chinese government instructed Alipay and Alibaba Cloud to develop the Health Code app into a nationwide platform – quickly launching in 100 cities within a week.[27] Officials stated on 24 February that about 90%– over 50 million people – in the Zhejiang Province (where Hangzhou is located)

had already downloaded the app. Tencent also released its version of the Health Code system through its WeChat app, which has more than one billion monthly users. The Health Codes were made mandatory for the Hubei province, where Wuhan is located, as it began easing lockdown measures.

Transparency related to the app's data practices has proven controversial, as there is a general lack of information on how user data is handled. Information on the system is mainly provided through external analysis, such as *The New York Times,* which discovered that users' location data is sent to the system's servers each time the user scans a QR code.[28] The Chinese government is also known to compel businesses, such as network operators, to provide GPS location data to track public movement, and there is concern that the Health Code apps allow even more accurate data to be retrieved from phones.[29] User data related to past purchases and chat history that the Alipay and WeChat apps store, is also of concern. Alibaba and Tencent deny that they provide the Chinese government with user data and state they only do so with user consent, though they also declined to describe exactly how the system works.[30]

Furthermore, no explanation or due process for appeal is given to users as to why they are assigned the colour codes, or when they will be reassigned a green code. This has led to some unease and concern, especially when glitches occur.[31] A user recently informed the *New York Times* for example, that her code was red for a single day before changing to green and that her multiple calls to the hotline were never answered.[32]

South Korea

South Korea uses a wide range of digital tools to facilitate contact tracing and movement tracking. The South Korean government released the "Self-Diagnosis Mobile Application" on 18 March 2020 for locals and foreigners entering South Korea to declare their health conditions over the preceding 14-day period.[33] From 1 April 2020 onwards, the app became mandatory and expanded in scope to monitor those who had close contact with COVID-19 patients.[34] It was also renamed the "Self-Quarantine Safety Protection App." A local government case officer checks-in with the user twice a day via the app (via phone calls if the user did not report through the app) to ensure that the user complies with quarantine and declaration requirements. Of note, the app collects GPS data to ensure that the user stays within their designated quarantine area. Those who fail to comply with the requirements may face up to a year of imprisonment or fines up to KRW 3 million (USD 2 444).

South Korea uses several measures to facilitate contact tracing. Upon confirmation of a COVID-19 infection, the government interviews the patient and if deemed necessary, gathers public CCTV recordings, credit card transactions, and GPS data from the patient's mobile phone to trace the patient's movement history.[35] The government then sends out emergency alert text messages through Korea's public warning system to inform citizens about the locations and movements of patients specific to the hour. Anonymised information on the patient is posted on the Ministry of Health and Welfare's website[36] and on the provinces' websites.[37]

The legal basis for these activities is a 2009 law updated in the wake of struggles to contain the MERS outbreak in 2015. The Infectious Disease Prevention and Control Act (IDPCA) was updated to empower public health authorities to collect private data from confirmed and potential patients without a

warrant.[38] Private telecommunications companies, national police agencies, and medical institutions are also specifically mandated to share such location data with health authorities. Such provisions in the IDPCA allowed the Korean authorities to rapidly conduct contact tracing to curb the outbreak.

South Korea's private sector developed several apps to facilitate contact tracing using such publicly available data. One such app is "Corona 100m" (Co100), which alerts users if they come within 100 metres of a location visited by an infected person. 1 million users had downloaded the app within 10 days of its launch.

South Korea's measures seem intrusive to privacy of many.[39] However, South Korea successfully managed to contain and limit the spread of COVID-19 without strict lockdown: shops, restaurants and leisure facilities had stayed open.[40] "Patient 31," a super spreader who ignored medical advice and led to a huge number of infections in Daegu city, strengthened the impetus for a strong enforcement and tracking system. Of note, Koreans were supportive of the strong approach with 80% of 1000 adults surveyed supported the proposal to use wristbands to enforce movement controls for those under self-quarantine, an implementation that had raised concerns over human rights.[41]

Singapore

Singapore was the first country in the world to roll-out a digital contact tracing app in response to COVID-19. The city-state benefitted from two critical factors. First, the country learned from previous experience dealing with the SARS outbreak in 2003. Second, the government has a strong team of software engineers working under its GovTech agency that was quickly able to ramp up app development. On 20 March 2020, the Ministry of Health and GovTech jointly launched their contact tracing app called "TraceTogether."

TraceTogether relies on BLE and only needs "Location Permissions" to know the relative distance of between users. Phones with the app installed will send each other a message that contains four pieces of information: a timestamp, Bluetooth signal strength, the phone's model, and a temporary identifier or device nickname. The app can identify people who have been in proximity, specifically 2m for at least 30 minutes. If someone with TraceTogether is diagnosed with COVID-19, he or she can simply upload their data to the Health Ministry, which will then be able to decrypt the information and begin contacting other TraceTogether users who have been in close contact of the confirmed COVID-19 case.

Nevertheless, the adoption rate has been quite low. One month after the launch, only 20% of the population or 1.1 million users have downloaded the app. The Minister for National Development, Lawrence Wong[42], and the Minister for Law and Home Affairs, K. Shanmugam, have come out to encourage people to download the app.[43] They need at least 3.2 million more downloads in order for the tool to be truly effective in digital contact tracing. By late May, 1.5million users[44] have downloaded the TraceTogether App, a 5% increase since its reported figure of 20% adoption rate since launch.

With the Circuit Breaker ending on 1 June, the Singapore government has structured re-opening of businesses as phases, implementing new digital requirements to enhance contact tracing. SafeEntry,[45] a

digital check-in system, is a mandatory requirement for those with physical business locations, to log check-in of visitors and employees. 16,000 venues have deployed [46] this system, and with further businesses and offices re-opening from 2 June, more will be implemented. Deployments on taxis will also be progressively implemented as part of the efforts. Food and beverage outlets (that are currently only open for delivery and/or takeaway) are not required to deploy SafeEntry for now. However, implementation is mandatory as part of workplace measures for retail businesses and restaurants.

To allay privacy concerns, the government has emphasized that the app does not collect or use any real-world geographic location. The data is only stored in the phones for only 21 days and will not be accessed unless they are identified as a close contact. Moreover, measures are in place to protect mobile numbers, such as pairing mobile numbers with a random ID.

Despite the public sector not being covered under the scope of Singapore's *Personal Data Protection Act*, the Singapore government had not yet made mandatory that citizens download the app. Recent cases of data breaches involving SingHealth do not spur confidence among citizens that their data will remain safely protected. But it may only be a matter of time before Singapore makes it compulsory for citizens to download the app. There are already comments[47] in the media that call for that such as Dr. Chia Shi-Lu, chairman of the Government Parliamentary Committee for Health, and news editor Irene Tham.[48]

Taiwan

The Taiwanese government has been praised for its COVID-19 containment strategy. While Taiwan has not mandated a nation-wide stay at home order, it has deployed mobile phone technologies to enforce quarantine guidelines at the municipality level. This strategy gave a large portion of the population the freedom to continue going to school and work. Big data analytics, coupled with Taiwan's national health database, aided the government in quickly identifying cases early and enforcing a strict 14-day "geofence" using mobile phone location tracking.

Taiwanese health officials, in coordination with local police departments, call and text those in quarantine twice a day via the Smart Care Management app 智慧關懷居家管理系統, which uses facial recognition and GPS technology to ensure patients are isolating safely.[49] Que Zhike 闕志克, the director of the Institute of Information and Communication Research of the Industrial Technology Research Institute, has said the system does not record data – assuring the public that images are only retained during the quarantine period.[50] Police are also using sim card tracking to ensure those who tested positive are complying with the stay in place order.

Further, in collaboration with Taiwan AI Lab, the government is developing a new app called Social Distance 社交距离, which uses Bluetooth technology to quickly determine where people have been.[51] According to a recent report[52], this app will be integrated with national 1968 Highway CCTV footage to alert people of crowded areas.[53] This app will also issue alerts when people are standing too close together, or otherwise not following social distancing guidelines.

To address privacy concerns, Taiwanese officials have confirmed the app will act only as an alert system and will not track citizens' movements or geolocation.[54] Further, data sharing will be voluntary, and all information will be anonymized and encrypted.

Social Distance app project manager, Jarvis Chan 詹仲昕, said the app will not require registration and will switch out temporary IDs every 15 minutes.[55] If a user tests positive for COVID-19, the app will obtain all past IDs from the patient with permission from the Taiwan Centres for Disease Control and send it out to those who contacted the patient. Taiwan's de-centralised approach will only store anonymous hashed ID data in the device for up to 28 days only.[56] Further, Jarvis Chan ensured the public that the app not only complies with obligations under the GDPR, but in fact goes further.

Japan

With confirmed coronavirus cases surging mid-April, Japanese Prime Minister Shinzo Abe declared a nationwide state of emergency 16 April[57] – urging[58] the public to reduce social contact by at least 70 percent and approving a USD 1.1 trillion stimulus package.[59] By early May total cases only reached 15 000, a number significantly lower than many of Japan's peers. However, like its neighbours, the Government of Japan is determined to release a contact tracing app to combat the growing pandemic and get the Japanese public back to work.

In coordination with the non-profit Code for Japan, the government is working to develop an app similar to Singapore's TraceTogether, which was launched 20 March.[60] In guidance released by Japan's Personal Information Protection Commission (PPC) 1 May, the PPC highlights the invaluable role contact tracing apps play in combatting COVID-19, while stressing the need to implement safeguards to protect user data.[61] The PPC explains that the decision to use these apps must be voluntary in nature and that users' privacy rights must be protected.

Rather than using geolocation information, which raises privacy concerns, Japan's app will rely on short-range Bluetooth communication.[62] Additionally, the software will encrypt data relating to the time, date, distance, and duration app users come in contact with others who have downloaded the app.[63] Then, when users have come within proximity of someone diagnosed with coronavirus, they will be alerted by a message. It is worth noting, that users will not be given details about *where* or *when* they encountered the potentially contagious person, ensuring anonymity. While technical details have yet to be shared publicly, the Government of Japan is expected to develop a centralised app, like the United Kingdom, rather than deploy the decentralised system Apple and Google have promoted.[64]

Further, contact tracing "business operators," handling personal information, must comply with Japan's Act on the Protection of Personal Information.[65] In accordance with the PPC's 1 May guidance, companies should:

1) Disclose how the user's personal information will be used and for what purposes (i.e. Including whether "special care-required personal information" will be shared with a third party) and obtain user consent
2) Refrain from the collection or sharing of data not necessary to combat COVID-19
3) Ensure data is deleted after a specified period has passed (and it is no longer needed from an epidemiological perspective)

4) Safeguard data and ensure the employees that handle data follow appropriate security measures; and

5) Establish a system to process and respond to user inquiries or complaints.[66]

Early May, with number of coronavirus-related deaths growing to nearly 600, Prime Minister Shinzo Abe extended the nationwide state of emergency through 31 May.[67]

India

India launched its contact tracing app, “Aarogya Setu" (“Bridge to Good Health”), on 2 April 2020.[68] The app was developed by the eGov Mobile Apps division of the National Informatics Centre (NIC). NIC is the organisation in charge of building and maintaining all government websites and apps.

The app tracks community transmission through the contact and travel history of individuals who are quarantined, infected, or suspected of being infected by COVID-19. The app uses a phone’s Bluetooth and location to generate a social graph of other users who had been in contact with the individual. This data is then matched and kept by the government. If a user had come near someone confirmed to be infected by COVID-19, the app alerts the user and asks them to get themselves tested.

The app has been criticised by the Internet Freedom Foundation (IFF) for failing to ensure the privacy of users, and the lack of transparency and accountability for the app. According to the IFF, there is no mention of which ministry or agency collects the data, and who has access to it. The privacy policy of the app also absolves the government of any liability in cases of unauthorized access or modification to user data. Furthermore, security researchers found a bug in the app that exposed some user data to YouTube. The bug was fixed in an update on 26 April 2020.[69]

Prime Minister Modi made an appeal in speeches and social media to download the app. PM Modi also indicated[70] that there is a possibility that the app could subsequently be used as an e-pass to facilitate travel from one place to another.[71] While the government initially also mandated all federal employees to download the app on their phones,[72] this has now been scaled back to a “best effort basis.”[73] As of 30 April, the app has been downloaded more than 75 million times.[74] As India has more than 550 million feature phones, which still use 2G and cannot run smartphone apps, the government plans to build a similar app for feature phones.[75]

Australia

Australia launched its voluntary COVIDSafe app on 26 April 2020 to expedite contact tracing efforts.[76] PM Scott Morrison said that the app was essential to help with contact tracing as Australia eases its COVID-19 restrictions. The app uses Bluetooth to conduct a digital handshake when other users' devices come within 1.5 metres, logging, and encrypting the other users' contact information for 21 days. If someone with the app tested positive for COVID-19 and agrees to share the phone data, the contact information will be transmitted to a central server for authorities to follow up on. COVIDSafe was inspired by Singapore's TraceTogether app and helps simplify contact tracing for government authorities to respond faster to contain community spread.

COVIDSafe saw quite a large success despite privacy concerns, with more than 2.4 million downloads within 24 hours of its launch. This puts it on track for the government's success marker of a 40% adoption rate (about 10 million people) for the app to be effective. Part of its success may also be attributed to how Australia frames the app as "essential" for Australia to relax COVID-19 restrictions.

To address Australians' privacy concerns, the government has given repeated assurances on how the app works and what it will not be used for (in response to rumours and fake news that it will be used to enforce movement restrictions). Clear documentation[77] on the governmental websites provide details on how the app works, and several privacy-focused reports,[78] policy documents[79] and determinations[80] have been published. The app also allows users to use a pseudonym instead of their real name. In addition, the Federal Health Minister has announced that the source code for COVIDSafe will be published for public scrutiny as requested by data protection groups.[81] Of note, Australia's news sources have also played a key role in combating fake news against COVIDSafe and promoting the app.

The initial legal basis and privacy requirements for the app was provided for by a determination of the Minister of Health under the Biosecurity Act. However the Australian Government has moved quickly to enshrine these protections within primary privacy law through the Privacy Amendment (Public Health Contact Information) Act 2020[82] which replaced the original determination. This bill was introduced into Parliament on 12 May 2020. The Bill specifies the circumstances in which the collection, use and/or disclosure of COVID app data is permitted.

Americas

Across the diverse states of North and South America, who have had very different experiences of the COVID-19 crisis to date, there have been fewer and less organized efforts by governments to develop contact tracing solutions. State, local, and national authorities are experimenting with using data to combat the pandemic and some have developed contact tracing approaches, however in general there is a lack of centralised efforts similar to national apps as in Asia and Europe. Especially in the United States, concerns about central government surveillance are also notable. However, as the epicentre of the global tech industry, US tech companies are leading in the development of technical tools that will arm governments around the world with the tools to do digital contact tracing while protecting privacy.

United States

The US response to COVID-19 generally is shaped by the diversity of local, state, and national actors relevant in the federal system of government. These entities play different roles, meaning that the situation can differ significantly between different regions. Digital contact tracing is no different. Given a severe lack of capacity in traditional contact tracing systems according to some experts, there are hopes that apps will help to allow rapid scaling of this capability.[83]

The US Centres for Disease Control and Prevention (CDC) published guidance on key features of contact tracing apps, focused on proximity-tracing functions based on Bluetooth or GPS and recommending anonymous and decentralised systems.[84] While it makes not explicit mention of the Apple/Google protocol, the CDC does cite the similar "PACT Protocol," developed by the Massachusetts Institute of Technology.[85]

Given that there are no signs the federal government is planning to run a central initiative, different states are pursuing their own systems. The state of Utah was an early jurisdiction out of the gate, having released its voluntary Healthy Together app for testing 22 April.[88] Their approach has drawn criticism because of its reliance on a broad set of individual mobile data, including not just Bluetooth proximity tracing but also geolocation and GPS data. The system will be neither anonymised nor decentralised, and state public health officials will have access to personally identifiable data.

In Hawaii, the Department of Health has contracted the development of an app to allow residents to upload their health information into a state-managed cloud server. Once the information is uploaded to the platform, workers are allowed limited access to contacts. Once one of these contacts has contracted the coronavirus, the state's Department of Health staff will contact others who may have been exposed. Those who may have been exposed are required to stay at home and monitor their health for 14 days after the phone call was received.

The private sector is also poised to take on a more prominent role in facilitating contact tracing. While Silicon Valley technology companies are developing and providing much of the digital capabilities used by public health authorities in the US and around the world, other less obvious sectors may come to play a prominent role as well – either voluntarily or mandatorily. As businesses seek ways to safely reopen workplaces, some large employers are cautiously exploring administering their own contact tracing systems focused on keeping their employees safe. Though the Apple/Google platform based on constant Bluetooth-based proximity signalling will only be open to public health authorities, other possible technical platforms in the market include smart badges, proximity censors, and Wi-Fi and Bluetooth triangulation data, among others. [89]

The aviation industry, which has been particularly devastated by the impact of COVID-19, is also on the front lines of private efforts. For several months, it has jousted with the government over the collection of passenger data related to COVID-19. The administration is seeking to deputize airlines to gather information from its customers through a CDC rulemaking process, something the airline

Salesforce and the Digital Transformation of Contact Tracing

Cloud software company Salesforce is also taking an active role in applying technology to enable contact tracing; however, they are pursuing a different path from Apple and Google. Though full technical details are yet to be released, the offering appears focused not on continuously tracing the movements of individuals, but on utilizing technology to supplement and increase the productivity of human labour performing contact tracing.

In announcing [86] the new product offering, Salesforce drew analogies between their well-known customer relationship manager (CRM) product, and called out three key functions it would be used to carry out: 1) help healthcare workers accelerate intake of patients; 2) help contact tracers identify risks to communities by tracing relationships between people; and 3) help authorities to reach out to those potentially exposed and set them up for ongoing monitoring and check ins.

Salesforce's offering is also different because it aims to provide tools to quickly scale contact tracing leveraging a diversity of actors such as private companies. Employers also face the challenge of keeping their employees safe and many are not waiting for federal government to do it for them. Salesforce's solutions are being used to support both private companies as well as public health authorities – such as New York City [87] where they are helping to set up a call centre, customer relationship, and case management system to support up to 2,500 New Yorkers running the system from June.

industry argues should be shouldered by the government. [90] A likely outcome of the stand-off is a new app which will gather additional biographic and contact information of international travellers to facilitate tracing by health authorities if needed.

However, serious problems of trust may impede uptake and usage of apps – even those administered by the government – undermining their effectiveness. According to a survey conducted by the University of Maryland and the Washington Post, Only 43% of US respondents trust Apple/Google to keep their data via such an app anonymous – versus 56% who don't.[91] Even for public health authorities, just 57% trust them with their data, versus 43% who would not.

Before the COVID-19 crisis, bipartisan progress towards a comprehensive federal privacy law had reached an impasse, as leadership of both parties in the Senate had staked out their favoured approaches and talks broke down. The impeachment proceedings against President Trump and the looming 2020 election had largely squashed any hope of further progress. However, despite the halting and uncoordinated government action on contact tracing, the prospect of using personal data, particularly tracking and tracing using mobile devices, by the government and private sector has already impacted the debate around federal privacy protections. It has provided grist to those pushing for a new law, leading to renewed calls for a unified federal standard.[92]

Senate Republicans took the first initiative, as a group of privacy leaders with otherwise different bills jointly introduced the COVID-19 Consumer Data Protection Act.[93] The bill would apply strict consent, notice, processing, retention, minimisation, and opt-out provisions on personal health data gathered in relation to the pandemic. Congressional Democrats have reacted with their own similar bill, the Public Health Emergency Privacy Act,[94] which would add stricter civil rights protections and clearer prohibitions on uses of data for certain activities like advertising.

Canada

Public health authorities at the federal, provincial, and municipal levels in Canada are either exploring or already implementing digital contact tracing measures to respond to COVID-19, renewing a national conversation about the privacy rights of Canadians.

In Canada, provinces and territories are generally responsible for providing direct health care services to Canadians and are therefore leading contact tracing efforts in the country, along with municipal health units in some cases. Health authorities have practiced manual contact tracing for decades, but as COVID-19 continues to spread and overburden public health departments, authorities are now exploring ways to enhance their contact tracing abilities with digital technologies. For example, British Columbia's chief medical officer of health told reporters the province is looking at how to use technology to bolster contact tracing capacity, while Ontario and Ottawa are considering options for contact tracing apps. The province of Newfoundland and Labrador is developing a mobile contact tracing app, and Alberta recently became the first province to adopt one, which uses Bluetooth to notify users if they may have been exposed to the virus.[95]

The federal government is also exploring contact tracing technology solutions, such as mobile location data and apps. According to Prime Minister Trudeau, the government has received proposals from several companies working on different models that might apply to Canada. Trudeau is also facing pressure from Ontario's premier to develop a national strategy that would coordinate the contact tracing work of the federal government, provinces, and territories.

Privacy concerns are top of mind as these developments unfold. Privacy advocates are speaking up, for example by calling on the country's telecommunications regulator to provide privacy protection guidelines for communications companies involved in contact tracing. Recognising the weight of the issue, Prime Minister Trudeau has stressed the importance of respecting Canadians' privacy when developing and implementing contact tracing solutions.[96] He and other federal and provincial government officials have also expressed a preference for voluntary measures over those that would penalise people for not participating.

Privacy commissioners across the country are also engaging on the issue. The national privacy commissioner has issued guidance and privacy principles for government officials considering measures to combat COVID-19 that have an impact on the privacy of Canadians, such as collecting location and other identifiable data.[97] Alberta's privacy commissioner issued a statement supporting the public health department's efforts to ensure their contact tracing app is voluntary, collects minimal information, uses decentralised storage, and allows users to control their use of the app.[98]

With more provincial governments, and potentially the federal government, poised to adopt digital contact tracing solutions to fight COVID-19, the privacy debate in Canada is expected to continue.

Mexico

On 31 March, lockdown in Mexico City was announced, shutting down all except essential shops and services.[99] As a part of the lockdown measures, telephone companies were providing access to cell phone antennas enabling the Digital Agency of Public Innovation (ADIP) to monitor the movement and contact between people in Mexico City. According to the Health Secretary Oliva López Arellano the aim of the measure was to identify whether people were complying with the lockdown restrictions.

The announcement of the measure was met with concern among the people and various civil society organisations due to the lack of information concerning the measure.[100] The proportionality and necessity of the measure was questioned and concerns of possible violations of right to privacy, freedom of communications and protection of personal data were raised.

In response to the reaction, The Digital Agency of Public Information on 1 April issued an informative note on collaboration with national telephone companies.[101] According to ADIP, only aggregated and anonymised information about users' location would be shared. The database where the information is collected, would not contain any type of information of private users or their behaviour. ADIP also noted that the sharing of information had started on the 25 March and occurs daily. The geolocation data would

allow for assessing changes in capacity in different areas daily and their relationship with the spread of the virus, allowing implementation of public policies to reduce the contagion rate of the virus and more effective responses.

Despite the additional information, the collection of data is still regarded as highly controversial. Concerns have been raised especially about the ambiguity of the measure coupled with contradictory and erratic communication. Additionally, NGO Article 19 has voiced concerns about the legal basis of the measure.[102]

To strengthen transparency and accountability of the ADIP's response to the pandemic, different databases have been made available in the City Government's data portal.[103]

Brazil

On 23 March, the City of Rio de Janeiro and telecom operator TIM signed an agreement to create a heat map of the city by using users' geolocation data.[104] The aim of the measure was to allow the local government to track whether people are complying with the lockdown measures.

On the 27 March, the Brazilian Institute of Consumer Protection (IDEC) announced that federal government had adopted the monitoring tool and in addition to TIM, four more telecom operators have agreed to provide geolocation data to the Ministry of Science, Innovation, Technology and Communication (MCTIC).[105] The objective of the data collection is to monitor the movement and agglomerations of people in the country in order to gather more information about the evolution of the pandemic. Considering that the five telecom operators account for 97.5% of all the of the 227.1 million mobile users in Brazil, the measure taken is rather extensive.

According to SindiTelebrasil (National Union of Telephony and Cellular and Personal Mobile Service Companies) the data collected from the users will be transferred to a public cloud, where it will be unified and anonymised.[106] In this way, it will not be possible to identify the person who is moving or leaving the house. The idea behind unifying and anonymising the data is to avoid violating the citizen's right to privacy.

Additionally, Brazilian Health Minister Luiz Henrique Mandetta had advocated for system where the telephone operators make individualised personal data available to health authorities to locate infected people. However, the Federal Attorney General and SindiTelebrasil have agreed that sharing data with this level of detail would violate the citizen's right to privacy.[107]

Furthermore, on 15 April, Brazil's National Telecommunications Agency (Anatel) announced its' position on tracking telecommunications users.[108] Anatel warned that the adoption of any measure must result from a motivated decision, with legal support and due transparency for the control bodies and for society and be proportional.

Despite several experts on data privacy and civil rights agreeing[109] that the use of anonymous data would not violate the right to privacy, the collection of anonymised data is still regarded controversial[110] and the legal basis of the measure have been scrutinised.

Colombia

On 9th of March, Colombian President Ivan Duque launched a mobile application to track COVID-19 cases in Colombia.[111] The free CoronApp-Colombia, developed partially by the National Health Institute of Colombia (INS), is focused on prevention of the virus. The application allows mobile users to register their health status and receive news and prevention advice. The app also contains various phone numbers that people can reach out in case of emergency and allows users to detect areas and people nearby that have a positive diagnosis of the virus, as a result of the app's Bluetooth-tracking. In the original launch, the application was available for download on Android, with availability for iOS added later.[112] The reaction by the Colombian government to the pandemic was very swift – at the time of the launch the whole country had only one confirmed case.[113]

The CoronApp-Colombia has raised some serious concerns regarding privacy.[114] Not long ago after the launch of the app, researchers found that the app was exposing user data by sending personal health information and personally identifiable information, such as passport numbers, passwords, and self-disclosed health information, allowing an attacker to filter the application's database. The Economic and Digital Transformation (MinTIC) Advisor Victor Muñoz stated with respect to the privacy concerns that the information collected will be encrypted and will be compliant with all cybersecurity and data protocols for data protection purposes.[115] Furthermore, the protocol of sending personal data would be improved and the data would be anonymised. In addition to the security vulnerabilities, there is ambiguity regarding how long the information collected through the CoronApp will be stored and what will happen to the data once the virus is over.[116]

The app has been and is marketed widely, the Minister of Information and Communication Technologies announced on 24 April that by downloading the CoronApp and registering, each user would receive 1GB of free data.[117] Seeing that the app is marketed aggressively and downloaded over million times solely for Android, guaranteeing the security of the app is of utmost importance.[118]

Middle East and Africa

South Africa

South Africa's largest telecom operator, Telkom, has joined hands with Samsung to assist the government in the fight against COVID-19 through contact tracing.[119] In mid-March, Samsung donated 1500 handsets to be distributed in the provinces that had been hardest hit by the virus (and where smartphone penetration was lowest). This initiative helped the mobile network operator Telkom in tracking infected people and identifying those that had been exposed to the virus. Telkom works with the country's National Institute for Communicable Diseases (NICD) and the Council for Scientific and Industrial Research (CSIR) in creating a database with insights into citizens' past movements and whereabouts.

To further contact tracing efforts, the South African government last month approached a group of researchers from the University of Cape Town (UCT) in order to develop a smartphone app that would help authorities track people who may be unaware that they have contracted COVID-19.[120] Named COVI ID, the app aims to use Bluetooth and geolocation to track and trace the movements of individuals, over the two-week period prior to them testing positive for the virus. The data is said to be stored on the smartphones of the individual in question rather than a centralised database belonging either to the government or the private sector.

Another platform mobilised by the government includes WhatsApp. At the outbreak of COVID-19, officials capitalised on the reach of the instant messaging app to mass deliver informative messages regarding the pandemic to millions of citizens in the country's five official languages.[121] South Africa's

Department of Health also created a WhatsApp helpline with the assistance of WHO and Praekelt, a non-profit organisation that uses mobile technology for the betterment of the poor.[122] The helpline data is updated with information from local and global news outlets as well as the latest WHO briefing in order to provide real-time updates. The service reached over 10 million users in just three days after it was first unveiled. The system uses AI to provide information on everything from viral symptoms to precautions and the location of nearby testing facilities and aims to dispel fake news that have gained traction.

Saudi Arabia

In early May, authorities in Saudi Arabia announced the trial launch of a new app called "Tawakkalna" aimed at managing the movement of people in the public and private sectors during the curfew imposed at night due to coronavirus.[123]

The app, launched by the Saudi Data and Artificial Intelligence Authority (SDAIA), will first be tested on a select group of employees working in the public and private sectors exempted from the curfew, employees of delivery apps, and individuals with medical appointments to enable them to apply and receive electronic permits. Through this new system, officials plan to allocate four hours per week for everyone who has applying to head out during curfew to secure their supplies at any time they want. Saudi Arabia partially lifted the curfew restrictions it imposed across the Kingdom starting on the 26 April while maintaining a full lockdown on Mecca and previously isolated neighbourhoods.[124]

It is not known whether the government is actively tracking the movements of individuals for the purposes of contact tracing. However, a recent leak of potential cell phone geolocation records related to a contact tracing product offered by the Israel-based NSO Group security firm indicates they may be running or testing such a programme.[125]

United Arab Emirates

In April, health authorities in Abu Dhabi announced the development of a national contact tracing app called TraceCOVID.[126] The app uses BLE technology to detect and identify other devices that have it installed. When in proximity of each other, both devices will exchange an encrypted Secure Tracing Identifier (STI) and store it on both devices. If one of the users is infected with coronavirus, authorities will be able to access the other user's data and timestamp to determine whether both need to be tested.

Officials have said that the app does not collect personally identifiable information and thus protects the privacy of personal information.[127] While it has not been made mandatory for Emirati residents to install the app as of now, officials are actively encouraging residents to use it.[128]

Iran

The government has recently introduced an app related to the services of this virus called ac19.ir.[129] The features of Corona Program, from the Ministry of Health, are:

- Information on the latest statistics and the number of patients and recovering people
- Educational videos on the prevention of the disease
- Information about the latest news about this disease in the country
- Test perform to assess your health
- News and updates from the Ministry of Health with regards to COVID19 and its management
- Information about medical centres in the provinces
- Announcement on the rumours

After its release, Iran's Health Ministry sent a mass SMS message to all Iranians urging them to install the app to check potential COVID-19 symptoms. The app would let users register using their phone number and then ask Iranians to answer a series of questions related to coronavirus symptoms.

The idea was to let Iranians determine if they had severe symptoms, to prevent citizens from needlessly flooding local hospitals. However, the app would also request access to real-time geo-location details, which it would immediately upload to a remote backend. Currently, while the app has been removed from the Play Store, the app is still being offered for download through the ac19.ir website and other third-party app stores.

In March, according to a tweet shared by MJ Azari Jahromi, Iran's Minister of Information and Communications Technology, the government has already collected location data points for more than four million Iranians with the help of the app.

Israel

Relatively early in this international spread of COVID-19, Israel adopted an aggressive stance to contact tracing, using mass gathering of geolocation data to prevent spread of the virus.

The Shin Bet internal security forces were granted emergency powers on 17 March by a Cabinet decision to facilitate contact tracing activities.[130] The Shin Bet was authorized to disclose phone geolocation records – typically gathered through telecommunications providers for counter-terrorism purposes – to public health authorities. In addition to tracking the prior movements of patients diagnosed with coronavirus and notifying those who came within close proximity, the Ministry of Health and the police would be able to use such data to monitor the current movements of those under quarantine, ensuring they do not violate their confinement.

The move, which was taken effectively without parliamentary approval, was controversial and reportedly opposed by the Privacy Protection Authority.[131] Civil rights groups swiftly rang the alarm bell, expressing concern at the broad sweep of data gathered, the method of approval of the measures, and the role of the security services in administering the system.[132]

At their enactment, Prime Minister Netanyahu billed the contact tracing measures as an effective way to counter the spread of the virus – citing the success of countries like Taiwan – "instead of isolating a whole country."[133] However, Israel like many other countries has still struggled to contain the spread of the virus, which ballooned from 300 cases at the measures' enactment to nearly 9 000 by early April, leading the Prime Minister to eventually order a full nation-wide lockdown on 6 April. [134]

While originally just supposed to last 30 days, authorities were extended to cover the state of emergency. However, the Knesset recently curtailed these powers, declining to extend their term further and effectively cutting off the police from geolocation data to enforce quarantine.[135] Israel's Supreme Court just threw a further wrench in the works, ordering that government authorities for the Shin Bet to gather and disclose such data must expire on 30 April in the absence of new legislation.[136] While the program has been provisionally extended until 26 May pending new legislation, it is not clear what powers the government will seek in a draft bill or what the Knesset may adopt.[137]

Looking Forward: Post-COVID Policy Impacts

Accelerating Digitalisation of Everyday Interactions

Technology is a critical disruptor as the world works to combat the COVID-19 crisis. From diverse contact tracing apps to innovative telehealth solutions, countries are adapting to a new digital normal. Consumers, businesses, and governments are shifting the ways in which they use technology, accelerating trends and shaping technology environments that will impact how data is collected and processed in a post-COVID-19 world.

Digital contact tracing, using various technologies, constitutes a massive expansion of the ways in which our everyday lives are monitored and quantified. Although we are already tracked online through every click and webpage, digital contact tracing, as it becomes more common, is bringing an awareness of being tracked in everyday life and our interactions in the physical world.

As communities, countries, and companies weigh the costs and benefits of 'returning to work', technology-enabled social distancing is of high importance. For those that do return to the office, application of radio-frequency identification (RFID), smart card, and similar touchless technologies are being adopted to securely digitalise user authentication and carry out contact tracing. The result for many

will be workplaces in which technology will increasingly intermediate interactions and be used to oversee and regulate behaviour.

More broadly in public spaces, biometrics are moving from national security surveillance to health surveillance. Facial recognition, retina scanning, palm vein scanning, and other touchless technologies became more prominent after the 9/11 terrorist attacks in security surveillance and access control. These same technologies are being re-tooled to provide instant temperature checks at airports, train stations, schools, and public gathering places – to protect public health and safety in a post COVID-19 world and will become part of the new normal.

Moving forward, the use of robotics and AI technologies will grow as businesses work to maximise distance between colleagues and customers. Several of these technologies, such as contactless payments, will also drive the digitalisation of the business-customer relationship – further increasing the individualised data available for digital contact tracing purposes.

With this increased dependence on and application of technology in our daily lives, it is important to consider the various risks and public policy challenges at play. It is also essential to remain cognizant of the trade-offs involved in the uses of these technologies between privacy, safety, and convenience.

Shifting the Privacy Debate

Digital contact tracing has created a major shift in how personal data is used in some jurisdictions, from well-established democracies such as Korea and Israel to more authoritarian states such as China and Iran. It has also provoked fear and sparked contentious debate across the globe, particularly in Europe.

For several years, the global privacy debate has been driven by private sector scandals and an EU-led approach to protecting consumer privacy through the private sector-focused General Data Protection Regulation. However, the COVID-19 crisis has shifted the conversation. Today, uses and potential abuses of data by governments are the centre of conversations, as public officials around the globe contemplate more expansive uses of data. Companies, by contrast, are positioning themselves as staunch champions of individual privacy, often forging stronger ties with former civil society critics.

In some countries, discussions of digital contact tracing and other measures to combat the virus have exposed the deficiencies of existing legal systems in ways that may spur more privacy protective action. In the United States, for example, the crisis has provoked new calls to pass a comprehensive national privacy law and resulted in new legislative bills focused on protecting privacy.

However, the crisis may result in wider and more fundamentally detrimental consequences for privacy. After the apparent success of efforts to combat the virus through the extensive use of personal data in countries like China and Korea, other governments may follow suit – resulting in a partial reversal of the decade long debate surrounding global personal data protection which has leaned towards restricting uses of personal data. As a result, the principle of data minimisation may lose some of its pre-eminence, as increased access to data is recognised as invaluable to protecting public health.

Building the Public Health Surveillance State

As this report shows, governments are working swiftly to expand the amount of health data available to them. While the scope of these efforts varies between countries, most are moving in the same direction – towards ever more collection and analysis of data. As a result, policy-makers are confronting challenges regarding the extent to which privacy protections that applied in the pre-COVID-19 era should remain applicable. While the EU is strenuously working to ensure the continued applicability of the GDPR, privacy concerns have generally become secondary to public health concerns.

How the global public views privacy protections may also be in flux. While scepticism towards government and private sector data processing remains high in some countries, the fear of a spreading pandemic may grow to outweigh reservations. While comprehensive comparative data is lacking, public opinion surveys in various countries tend to indicate a degree of willingness to use voluntary apps and sacrifice some level of privacy for public health purposes.[138] However, other surveys in the US have indicated scepticism,[139] while France and other Western countries have seen contentious political controversies around contact tracing.[140] These indicate that there may in fact be significant public resistance to government overreach in certain countries.

Does extensive collection and analysis of personal health data by the state become the new normal, in the same manner that extensive state surveillance became largely normalised after traumatic terrorist attacks in the West in the early 2000s?

The experience of South Korea indicates that perhaps it can. The country struggled to contain a previous disease outbreak several years ago, leading to the adoption of a law which enabled sweeping government access to personal data despite having one of the strictest privacy regimes in the world. These statutory authorities have now been exercised to the fullest, underpinning Seoul's contact tracing programme, which has shown real results and enjoy public support. Countries that are interested in doing likewise face not just the technical challenge of building effective digital contact tracing systems, but of constructing a thoughtful legal framework that balances public health needs with data protection concerns, as well as the compliance environment to ensure clear accountability and obligations for public and private sector actors involved.

Public Health and International Privacy Interoperability

This report details the different ways that governments are approaching contact tracing, as well as the different legal and political contexts underlying those decisions. As governments continue to grapple with the crisis and adapt solutions to mitigate it, they will likely continue to pursue and codify in law divergent approaches, rooted in different political systems and values related to privacy and public health. These different national approaches to contact tracing may create a new fault line in international privacy interoperability.

Throughout this crisis, the EU has generally sought to ensure the continued application of the GDPR without infringement, abridgement, or amendment. However, many other governments around the world have taken a far less measured approach, taking steps that go beyond the existing law or seeking changes to existing frameworks.

European privacy authorities have been much less enthusiastic about adopting extraordinary measures. Europe has signalled it is closely watching the measures taken by others, an attitude which may have long term ramifications for the EU's policy approach to international transfers of personal data. Overly aggressive digital contact tracing that uses personal data in ways significantly at odds with the spirit of the EU GDPR could have serious consequences for data flows. South Korea, with its aggressive contact tracing programme, is currently in the process of negotiating an adequacy agreement with the EU, while Japan recently concluded one. Much closer to home, the United Kingdom is also pressed to complete the adequacy process with the European Commission by the end of 2020 or risk new barriers to EU-UK cross border data flows. These countries could face questions regarding the privacy protections baked into their contact tracing choices.

We have yet to see whether the European Commission or the European Data Protection Board will press European standards in relation to public health around the world, but the implications for international digital trade and global privacy norms could be significant if they do. Without better mechanisms to manage these legal differences, uses of personal data for public health purposes could become a new irritant in international commerce, as differing legal standards create barriers to seamless data flows or national mandates impose new technical requirements and compliance costs on private companies.

Conclusion

Countries are deploying a diverse set of technical tools and policy responses to combat the COVID-19 crisis. However, as governments work against the clock, privacy has largely taken a back seat. While some policy-makers are willing to make this trade off, there may be signs of a growing public backlash in some countries. How this dynamic will play out in the long term is difficult to predict, though it is likely that governments' push for expanded use of personal data will to some extent become the new normal.

Further, we do not yet know how effective different kinds of contact tracing solutions will be. Whether more limited tools, which provide stronger privacy protections, will lead to successful outcomes in the near term, remains to be seen. Their efficacy will depend not only on the technical performance of the technology used, but on mass adoption of these opt-in, consent-based systems. The success – or failure – of more privacy-protective approaches, like Bluetooth Low Energy (BLE) proximity tracing, will significantly impact how countries decide to resolve the privacy versus security dilemma.

If Bluetooth-based approaches fail to deliver workable tools for governments, more expansive – and less voluntary – approaches to digital contact tracing will likely be adopted. The public health surveillance state may be with us for some time to come as a marker of good governance. If so, policymakers face significant challenges to construct corresponding trusted governance frameworks that provide meaningful privacy protections and control potential abuses by the state.

Whatever path countries take, governments and stakeholders face a need to continually balance data protection and privacy concerns with public health measures. To build effective solutions and attain the full benefits of technology, these need to build trust with transparent, equitable legal regimes and inclusive dialogue.

Companies must continue working as good faith partners and expert advisors. Due to the central role of technology provided by the private sector in digital contact tracing, their enabling role – through technical expertise, mobilising resources, and providing expert advice – is indispensable.

While the costs of poor governance and eroding trust are high, so too are the potential societal benefits of getting it right. With thoughtful and inclusive policy responses to guide the deployment of digital contact tracing, technology can continue to enhance welfare – health, wealth, and rights.

About Access Partnership

Access Partnership is the world's leading technology public policy consulting firm. Operating in 16 languages across 6 global offices, we monitor and analyse global trends for the risks and opportunities they create for business and governments, drawing on long experience of international public policy and technologies new and old.

Our clients include some of the world's largest governments, manufacturers, services companies, telecommunications network operators, and international organisations. Our team uniquely mixes policy and technical expertise, with staff members drawn from industry, public affairs agencies, government agencies, private legal practice and technical assistance programmes.

From navigating a changing global privacy regime in the age of COVID-19, to ensuring countries have access to the innovative tools and digital solutions needed to combat the crisis, Access Partnership is here to support you. Whether a government stakeholder, industry leader, or emerging start-up, our team is well-equipped to help partners navigate an evolving regulatory landscape and shape smart, forward-thinking technology policy outcomes during the COVID-19 crisis and beyond.

Endnotes

[1] Bettinger, Pete and Merry, Krista. "Smartphone GPS accuracy study in an urban environment." *PLoS ONE*. 18 July 2019. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0219890>.

[2] Apple Newsroom. "Apple and Google partner on COVID-19 contact tracing technology." 10 April 2020 <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-COVID-19-contact-tracing-technology/>.

[3] Silver, Laura. "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally." *Pew Research Center.* 5 February 2019. <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>.

[4] PEPP-PT. "Pan-European Privacy-Preserving Proximity Tracing." 19 May 2020. <https://www.pepp-pt.org/>.

[5] Stolton, Samuel. "Digital Brief: PEPP-PT – The Inside Story." *Euractiv.* 29 April 2020. <https://www.euractiv.com/section/digital/news/digital-brief-pepp-pt-the-inside-story/>.

[6] Scott, Mark et al. "How Google and Apple outflanked governments in the race to build coronavirus apps." *Politico.* 15 May 2020. <https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/>.

[7] European Commission. "Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection." *Official Journal of the European Union.* 17 April 2020. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=EN>.

[8] 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." 21 April 2020. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_COVID_with_annex_en.pdf>.

[9] Ratti, Francesca et al. "By surrendering to autocracy in the fight against COVID-19, Hungary poisons European ideals." *Euractiv.* 20 April 2020. <https://www.euractiv.com/section/future-eu/opinion/by-surrendering-to-autocracy-in-the-fight-against-COVID-19-hungary-poisons-european-ideals/>.

[10] "Coronavirus Tracking UK Public Perception." *Ipsos MORI.* 1 May 2020. <https://www.ipsos.com/sites/default/files/2020-04/coronavirus-COVID-19-infographic-ipsos-mori.pdf>.

[11] Lomas, Natasha. "Germany ditches centralised approach to app for COVID-19 contacts tracing." *TechCrunch.* 27 April 2020. <https://techcrunch.com/2020/04/27/germany-ditches-centralised-approach-to-app-for-COVID-19-contacts-tracing/?guccounter=1>.

[12] Busvine, Douglas and Rinke, Andreas. "Germany flips to Apple-Google approach on smartphone contact tracing." *Reuters.* 26 April 2020. <https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-on-smartphone-contact-tracing-backs-apple-and-google-idUSKCN22807J>.

[13] Chazan, Guy and Miller, Joe. "Contact-tracing apps raise privacy concerns in Germany." *Financial Times.* 16 April 2020. <https://www.ft.com/content/32b6a360-3e22-47a3-ace5-60f42cc6b42d>.

[14] Deutsche Telekom AG and SAP SE. "Corona-warn-app / cwa-documentation." *GitHub.* 2020. <https://github.com/corona-warn-app/cwa-documentation>.

[15] "Decentralised Privacy-Preserving Proximity Tracing – Documents." *GitHub*. April 2020. <https://github.com/DP-3T/documents>.

[16] TCN Coalition. "A Global Coalition for Privacy-First Digital Contact Tracing Protocols to Fight COVID-19." 10 April 2020. <https://tcn-coalition.org/>.

[17] Apple and Google. "Privacy-Preserving Contact Tracing." *Apple.* <https://www.apple.com/COVID19/contacttracing/>.

[18] Asher Hamilton, Isobel. "France attacks Apple for not helping to build its contact-tracing app." *Business Insider.* 6 May 2020. <https://www.businessinsider.com/france-attacks-apple-contact-tracing-app-2020-5?r=US&IR=T>.

[19] Sudouest avec AFP. “Coronavirus : Why the "StopCOVID" application, used to track the sick, will be subject to debate.” *Sud Ouest.* 8 April 2020. <https://www.sudouest.fr/2020/04/08/coronavirus-stopCOVID-l-application-qui-alertera-en-cas-de-contact-avec-un-malade-7395875-10861.php>.

[20] Lamon, Bernard. “Opinion | StopCOVID: GDPR authorizes everything and prohibits nothing.” *Les Echos.* 4 May 2020. <https://www.lesechos.fr/idees-debats/cercle/opinion-stopCOVID-le-rgpd-autorise-tout-et-ninterdit-rien-1200111>.

[21] Reuters Staff. “Coronavirus: "StopCOVID" application may not be ready on May 11." *Reuters.* 17 April 2020. <https://fr.reuters.com/article/topNews/idFRKBN21Z1I3>.

[22] The National Assembly and the Senate. “Emergency Law n ° 2020-290 of March 23, 2020 to deal with the COVID-19 epidemic (1).” *The State of Health Emergency.* 23 March 2020. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041746313&dateTexte=20200515>.

[23] Guarantor for the Protection of Personal Data. “Opinion on the regulatory proposal for the provision of an application aimed at tracking contagions from COVID-19.” 29 April 2020. <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9328050>.

[24] Ministry for Technological Innovation and Digitization. “An update on the digital contact tracing application for the coronavirus emergency.” 21 April 2020. <https://innovazione.gov.it/un-aggiornamento-sull-applicazione-di-contact-tracing-digitale-per-l-emergenza-coronavirus/>.

[25] “Alipay health code landed in 100 cities in 7 days, digital epidemic prevention ran out of ‘Chinese speed.’” *Xinhuanet.* 19 February 2020. <http://www.xinhuanet.com/tech/2020-02/19/c_1125596647.htm>.

[26] Ibid.

[27] Jianguo, Meng et al. “China promotes health codes to monitor outbreaks and people.” *The New York Times.* 3 March 2020. <https://cn.nytimes.com/china/20200303/china-coronavirus-surveillance/>.

[28] Mozur, Paul et al. “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags.” *The New York Times.* 1 March 2020. <https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html?_ga=2.2528374.733865683.1588601533-1883129577.1588601533>.

[29] Yang, Yuan et al. “China, coronavirus and surveillance: the messy reality of personal data.” *Financial Times.* 2 April 2020. <https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca>.

[30] Mozur, Paul et al.

[31] Jianguo, Meng et al.

[32] Mozur, Paul et al.

[33] Self-diagnosis Mobile App. *Ministry of Health and Welfare of the Republic of Korea.* 18 March 2020. <http://overseas.mofa.go.kr/ke-en/brd/m_10538/view.do?seq=761314>.

[34] “Mandatory Installation of new ‘Self Quarantine Safety Protection App’ for all who enter Korea.” *Ministry of Health and Welfare of the Republic of Korea.* 31 March 2020. <http://overseas.mofa.go.kr/ke-en/brd/m_10538/view.do?seq=761319&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=>.

[35] Korean Government’s Response System”. *Ministry of Health and Welfare of the Republic of Korea.* 25 February 2020. <http://ncov.mohw.go.kr/en/baroView.do?brdId=11&brdGubun=111&dataGubun=&ncvContSeq=&contSeq=&board_id=>.

[36] Domestic occurrence status. *Ministry of Health and Welfare of the Republic of Korea.* 18 May 2020. <http://ncov.mohw.go.kr/bdBoardList_Real.do>.

[37] COVID-19. *Seoul Metropolitan Government*. Accessed 18 May 2020. <http://www.seoul.go.kr/coronaV/coronaStatus.do>.

[38] Infectious Disease Control and Prevention Act. *Korea Law Translation Center.* 2 December 2016. <https://elaw.klri.re.kr/eng_service/lawView.do?hseq=40184&lang=ENG>.

[39] A Jo, Eun. "South Korea's Experiment in Pandemic Surveillance." *The Diplomat.* 13 April 2020. <https://thediplomat.com/2020/04/south-koreas-experiment-in-pandemic-surveillance/>.

[40] "First person: South Korea's COVID-19 success story." *UN News.* 1 May 2020. <https://news.un.org/en/story/2020/05/1063112>.

[41] Yonhap. "S. Korea to use electronic wristbands on violators of self-isolation rules: PM." *Korea Herald.* 11 April 2020. <http://www.koreaherald.com/view.php?ud=20200411000043>.

[42] Chong, Clara. "About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong". *The Straits Times.* 1 April 2020. <https://www.straitstimes.com/singapore/about-one-million-people-have-downloaded-the-tracetogether-app-but-more-need-to-do-so-for>.

[43] Yong, Charissa. "Coronavirus: Contact-tracing apps key to country opening up again, says Shanmugam." *The Straits Times.* 3 May 2020. <https://www.straitstimes.com/world/united-states/contact-tracing-apps-key-to-country-opening-up-again-shanmugam>.

[44] Singaporean contact tracing app. *TraceTogether.* 7 May 2020. <https://www.tracetogether.gov.sg/>.

[45] SafeEntry. "Places where SafeEntry must be deployed." 12 May 2020. <https://www.safeentry.gov.sg/deployment>.

[46] CAN. "COVID-19: SafeEntry digital check-in system deployed to more than 16,000 venues." 9 May 2020. <https://www.channelnewsasia.com/news/singapore/COVID-19-safe-entry-digital-checkin-deployed-16000-venues-12717392>.

[47] Mohamad Rosli, Tatiana. "TraceTogether app should be mandatory for all: Experts." *The New Paper.* 4 May 2020. <https://www.tnp.sg/news/singapore/tracetogether-app-should-be-mandatory-all-experts>.

[48] Tham, Irene. "No other way but to make use of TraceTogether mandatory." *The Straits Times.* 1 May 2020. <https://www.straitstimes.com/singapore/no-other-way-but-to-make-use-of-tracetogether-mandatory>.

[49] Atkinson. "ITRI 's smart care home management system helps to improve care positioning from 100 meters to 10 meters." *TechNews.* 22 April 2020. <https://technews.tw/2020/04/22/itri-epidemic-prevention-app-launch/>.

[50] Jingyuan, Gao. "Tracing the tired grassroots of home quarantine? This mobile app automates the epidemic prevention work of the Lichang." *Business Next.* 22 April 2020. <https://www.bnext.com.tw/article/57397/itri-home-quarantine-system>.

[51] Taiwan Social Distancing App. *AI Labs.tw.* 18 May 2020. <https://covirus.cc/social-distancing-app-intro.html>.

[52] Minfeng, Chen. "Taiwan completes the development of social hotspot apps to warn that social distance is too close to record contact history." *RFI.* 12 April 2020. <http://www.rfi.fr/cn/%E6%B8%AF%E6%BE%B3%E5%8F%B0/20200412-%E5%8F%B0%E6%B9%BE%E5%AE%8C%E6%88%90%E7%A4%BE%E4%BA%A4%E7%83%AD%E7%82%B9app%E5%BC%80%E5%8F%91%E5%8F%AF%E8%AD%A6%E7%A4%BA%E7%A4%BE%E4%BA%A4%E8%B7%9D%E7%A6%BB%E8%BF%87%E8%BF%91%E8%AE%B0%E5%BD%95%E6%8E%A5%E8%A7%A6%E5%8F%B2>.

[53] 1968 Highway CCTV. Accessed 18 May 2020. <https://1968.freeway.gov.tw/>.

[54] Naixin, Pan. "Social distance APP exposure privacy? Taiwan AI Lab: stricter than EU regulations." *United News.* 25 April 2020. <https://udn.com/news/story/120940/4517830>.

[55] Ibid.

[56] Taiwan Social Distancing App.

[57] "Declaration of a State of Emergency in response to the Novel Coronavirus Disease." *Prime Minister of Japan and His Cabinet.* 16 April 2020. <https://japan.kantei.go.jp/ongoingtopics/_00020.html>.

[58] "Press Conference by the Prime Minister regarding the Novel Coronavirus." *Prime Minister of Japan and His Cabinet.* 17 April 2020. <https://japan.kantei.go.jp/98_abe/statement/202004/_00002.html>.

[59] "Emergency Economic Measures for Response to COVID-19 to protect the lives and lifestyles of the public and move toward economic recovery". *Prime Minister of Japan and His Cabinet.* 20 April 2020. <http://japan.kantei.go.jp/ongoingtopics/_00019.html>.

[60] Code for Japan. Accessed 18 May 2020. <https://www.code4japan.org/>.

[61] "Personal Information Protection Commission's view on effective use of contact tracing App to help deal with Coronavirus disease (COVID-19)." *Personal Information Protection Commission.* 1 May 2020. <https://www.ppc.go.jp/files/pdf/information_20200501.pdf>.

[62] "Notification of contact with infected person is also ... Is the data utilization to the overthrow corona the savior?" *Newswitch.jp.* 20 April 2020. <https://newswitch.jp/p/21902>.

[63] "Japanese government to release coronavirus contact-tracing app in May." *The Japan Times.* 29 April 2020. <https://www.japantimes.co.jp/news/2020/04/29/national/japanese-government-release-coronavirus-contact-tracing-app-may/#.XsKg8GhKhPZ>.

[64] Burgess, Matt. "Everything you need to know about the NHS COVID-19 tracking app." *Wired.* 4 May 2020. <https://www.wired.co.uk/article/nhs-COVID-19-tracking-app-contact-tracing>.

[65] "Act on the Protection of Personal Information Act No. 57 of (2003)." Accessed 18 May 2020. <https://www.jetro.go.jp/ext_images/usa/APPI.pdf>.

[66] "Personal Information Protection Commission's view on effective use of contact tracing App to help deal with Coronavirus disease (COVID-19)." *Personal Information Protection Commission.* 1 May 2020. <https://www.ppc.go.jp/files/pdf/information_20200501.pdf>.

[67] "New Coronavirus Infectious Disease Control Headquarters (33rd)." *Prime Minister of Japan and His Cabinet.* 4 May 2020. <https://www.kantei.go.jp/jp/98_abe/actions/202005/04corona.html>.

[68] Aarogya Setu Mobile App. *Government of India.* Accessed 18 May 2020. <https://www.mygov.in/aarogya-setu-app/>.

[69] "Aarogya Setu app exposed some user data to YouTube, flaw fixed now." *India Today.* 27 April 2020. <https://www.indiatoday.in/technology/news/story/aarogya-setu-app-exposed-some-user-data-to-youtube-flaw-fixed-now-1671747-2020-04-27>.

[70] "Narendra Modi asks citizens to download Aarogya Setu app; here's how to download and use it." *Firstpost.com.* 14 April 2020. <https://www.firstpost.com/health/narendra-modi-asks-citizens-to-download-aarogya-setu-app-heres-how-to-download-and-use-it-8258431.html>.

[71] "PM Modi Says Aarogya Setu App is Critical in The Fight Against COVID: Here is How it Works." *New18.com.* 14 April 2020. <https://www.news18.com/news/tech/pm-modi-says-aarogya-setu-app-is-critical-in-the-fight-against-COVID-here-is-how-it-works-2576857.html>.

[72] Bhalla, Abhishek. "Centre makes Arogya Setu app must for all central govt employees." *India Times.* 29 April 2020. <https://www.indiatoday.in/india/story/centre-makes-arogya-setu-app-must-for-all-central-govt-employees-1672415-2020-04-29>.

[73] Government of India. "No. 40-3/2020-DM-I(A)." Ministry of Home Affairs. 17 May 2020. < https://www.thehindu.com/news/resources/article31608347.ece/binary/MHAOrderdatedMay17-GuidelinesofLockdownextension.pdf >.

[74] Harb, Robbie. "India to build contact-tracing app for feature phones that still use 2G, don't have Bluetooth and can't run apps." *The Register.* 30 April 2020. <https://www.theregister.co.uk/2020/04/30/india_to_develop_contact_tracing_for_feature_phones/>.

[75] Shankar Prasad, Ravi. *Twitter.com.* 28 April 2020. <https://twitter.com/rsprasad/status/1255070654795091968>.

[76] "COVIDSafe: New app to slow the spread of coronavirus." *Prime Minister, Minister for Health, Minister for Government Services, Chief Medical Officer.* 26 April 2020. <https://www.pm.gov.au/media/COVIDsafe-new-app-slow-spread-coronavirus>.

[77] COVIDSafe app. *Australian Department of Health.* Accessed 18 May 2020. <https://www.health.gov.au/resources/apps-and-tools/COVIDsafe-app#get-the-app>.

[78] COVIDSafe Application Privacy Impact Assessment. *Australian Department of Health.* Accessed 18 May 2020. <https://www.health.gov.au/resources/publications/COVIDsafe-application-privacy-impact-assessment>.

[79] Privacy policy for COVIDSafe app. *Australian Department of Health.* Accessed 18 May 2020. <https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-COVIDsafe-app>.

[80] Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020*. Australia Federal Register of Legislation.* 25 April 2020. <https://www.legislation.gov.au/Details/F2020L00480>.

[81] Lane, Sabra. "Federal Health minister says Govt will release COVIDSafe source code." *ABC News.* 27 April 2020. <https://www.abc.net.au/radio/programs/am/heath-minister-says-govt-will-release-COVIDsafe-source-code/12187634>.

[82] Parliament of Australia. "Privacy Amendment (Public Health Contact Information) Act 2020." Federal Register of Legislation. 15 May 2020. <https://www.legislation.gov.au/Details/C2020A00044>.

[83] Timm, Jane C. "Fact check: Trump says the U.S. ready to contain COVID-19 with contact tracing. Experts disagree." *NBC News.* 30 April 2020. <https://www.nbcnews.com/politics/politics-news/fact-check-trump-says-u-s-ready-contain-COVID-19-n1195621>.

[84] "Preliminary Criteria for the Evaluation of Digital Contact Tracing Tools for COVID-19." *Center for Disease Control.* Accessed 18 May 2020. <https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/prelim-eval-criteria-digital-contact-tracing.pdf>.

[85] PACT: Private Automated Contact Tracing. *Massachusetts Institute of Technology.* Accessed 18 May 2020. <https://pact.mit.edu/>.

[86] Seaman, Rob. "Contact Tracing." *Salesforce.* 5 May 2020. <https://salesforce.vidyard.com/watch/UoTJaLdpVDbzaRp8DHMRj2?>.

[87] Higgins-Dunn, Noah and Feur, William. "New York City partners with Salesforce on coronavirus contact tracing program, mayor says." CNBC. 8 May 2020. <https://www.cnbc.com/2020/05/08/new-york-city-partners-with-salesforce-on-coronavirus-contact-tracing-program-mayor-says.html>.

[88] Khalid, Amrita. "Utah's new COVID-19 contact tracing app will track user locations." *Quartz.* 23 April 2020. <https://qz.com/1843418/utahs-new-COVID-19-contact-tracing-app-will-track-user-locations/>.

[89] "As workplaces slowly reopen, tech companies smell a new multibillion-dollar opportunity: Helping businesses trace coronavirus." *CNBC*. 10 May 2020. < https://www.cnbc.com/2020/05/10/coronavirus-tracing-for-workplaces-could-become-new-tech-opportunity.html>

[90] "Airlines, government at odds over passenger 'contact tracing'." *Roll Call*. 14 May 2020. < https://www.rollcall.com/2020/05/14/airlines-government-at-odds-over-passenger-contact-tracing/>.

[91] "Washington Post-University of Maryland national poll, April 21-26, 2020." *Washington Post.* 5 May 2020. <https://www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/3583b4e9-66be-4ed6-a457-f6630a550ddf/?itid=lk_inline_manual_3>.

[92] McMorris Rogers, Cathy. "Coronavirus and Privacy Protection." *Morning Consult.* 7 May 2020. <https://morningconsult.com/opinions/coronavirus-and-privacy-protection/?mkt_tok=eyJpIjoiTjJaaU5EYzNObUprWW1OayIsInQiOiJ1RlFxdTJLWGRxaDVyRHhDWm5YMkpFOVNWRUlmM3djQmRMM2E1c1lBd0RRWXpCSGNJNzRITnBGbXIrWVwvT2g2enNUOEJsZHZaZVF6ZG52K0dLVEZsZzNIYzhkTmIrRVVmNFJ4aExLVG9NWTlqWEVCdjYzMUhNMkVodXB6Q25rRVMifQ%3D%3D>.

[93] COVID–19 Consumer Data Protection Act of 2020. 116th Congress 2nd Session. <https://www.commerce.senate.gov/services/files/A377AEEB-464E-4D5E-BFB8-11003149B6E0>.

[94] Public Health Emergency Privacy Act. 116th Congress 2nd Session. <https://delbene.house.gov/uploadedfiles/public_health_emergency_privacy_act_-_as_introduced.pdf>.

[95] "ABTraceTogether privacy statement." *Government of Alberta.* Accessed 18 May 2020. <https://www.alberta.ca/ab-trace-together-privacy.aspx>.

[96] "PIAC Calls for CRTC Oversight of Contact-Tracing Apps and Networks." *Public Interest Advocacy Centre.* 4 May 2020. <https://www.piac.ca/our-specialities/piac-calls-for-crtc-oversight-of-contact-tracing-apps-and-networks/>.

[97] "A Framework for the Government of Canada to Assess Privacy-Impactful Initiatives in Response to COVID-19." *The Office of the Privacy Commissioner of Canada.* April 2020. <https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/fw_COVID/>.

[98] "Commissioner Comments on Alberta's Contact Tracing App." *Office of the Information and Privacy Commissioner of Alberta.* 1 May 2020. <https://www.oipc.ab.ca/news-and-events/news-releases/2020/commissioner-comments-on-alberta%E2%80%99s-contact-tracing-app.aspx>.

[99] "Closing of shopping centres due to health emergency." *Government of Mexico City.* 31 March 2020. <https://cdmx.gob.mx/portal/articulo/cierre-de-centros-comerciales-por-emergencia-sanitaria>.

[100] "Use of technologies as a measure against the spread of COVID-19 must be implemented with strict adherence to human rights." *Articulo19.org.* 2 April 2020. <https://articulo19.org/uso-de-tecnologias-como-medida-contra-la-propagacion-de-COVID-19-debe-implementarse-con-estricto-apego-a-los-derechos-humanos/>.

[101] "Information note on collaboration with national mobile phone operators before COVID-19." *Government of Mexico City.* 1 April 2020. <https://adip.cdmx.gob.mx/comunicacion/nota/nota-informativa-sobre-la-colaboracion-con-los-operadores-nacionales-de-telefonia>.

[102] "Use of technologies as a measure against the spread of COVID-19 must be implemented with strict adherence to human rights"

[103] "Section COVID-19 presented within the open data portal of Mexico City to strengthen transparency and accountability in the response to the pandemic." *Government of Mexico City.* 27 April 2020. <https://adip.cdmx.gob.mx/comunicacion/nota/presentan-seccion-COVID-19-dentro-del-portal-de-datos-abiertos-de-la-ciudad-de-mexico-para-fortalecer-la-transparencia-y-rendicion-de-cuentas-en-la-respuesta-la-pandemia>.

[104] Do Amaral, Bruno. "Coronavirus: TIM and Rio City Hall sign agreement to collect displacement data." *Teletime.com.br*. 23 March 2020. <https://teletime.com.br/23/03/2020/coronavirus-tim-e-prefeitura-do-rio-assinam-acordo-para-coletar-dados-de-deslocamento/>.

[105] "To combat COVID-19, federal government will monitor your cell phone." *Instituo Brasileiro de Defesa do Consumidor.* 13 April 2020. <https://idec.org.br/idec-na-imprensa/para-combater-COVID-19-governo-federal-vai-monitorar-seu-celular>.

[106] Ibid.

[107] Magenta, Matheus. "Coronavirus: Brazilian government to monitor cell phones to contain pandemic." *BBC News.* 3 April 2020. <https://www.bbc.com/portuguese/brasil-52154128>.

[108] "Anatel's position regarding the use of tracking telecommunications users as part of measures to combat the COVID-19 pandemic." *Anatel.* 15 April 2020. <https://www.anatel.gov.br/institucional/mais-noticias/2561-posicionamento-da-anatel-a-respeito-da-utilizacao-de-rastreamento-de-usuarios-de-telecomunicacoes-no-ambito-de-medidas-no-combate-a-pandemia-de-COVID-19>.

[109] "To combat COVID-19, federal government will monitor your cell phone."

[110] "Coronavirus: Brazilian government to monitor cell phones to contain pandemic."

[111] Gamba, Laura. "Colombian president launches app to track COVID-19." *Anadolu Agency.* 9 March 2020. <https://www.aa.com.tr/en/americas/colombian-president-launches-app-to-track-COVID-19/1759011>.

[112] Moss, Loren. "Colombia Minsalud Health Ministry Website Collapses Under Coronavirus Traffic." *Finance Colombia.* 11 March 2020. <https://www.financecolombia.com/colombia-minsalud-health-ministry-website-collapses-under-coronavirus-traffic/>.

[113] "Colombian president launches app to track COVID-19."

[114] Labarthe, Stéphane and Velásquez, Andrés. "CoronApp, Medellín Take care of me and CaliValle Corona to the laboratory -Or how CoronApp is hacked without even trying." *Karisma.* 17 April 2020. <https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/>.

[115] "CoronApp, the application that saves lives." *Colombia Ministry of Information and Communications Technologies.* 14 April 2020. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/126573:CoronApp-la-aplicacion-que-salva-vidas>.

[116] "CoronaApp will be key to go out to the streets again while the emergency lasts." *El Tiempo.* 24 April 2020. <https://www.eltiempo.com/tecnosfera/apps/coronavirus-en-colombia-coronapp-servira-como-pasaporte-en-las-calles-484266>.

[117] "Mobile internet and free voice minutes during one month, to take care of your health." *Colombia Ministry of Information and Communications Technologies*. 24 April 2020. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/135698:Internet-movil-y-minutos-de-voz-gratis-durante-un-mes-para-cuidar-tu-salud>.

[118] Labarthe, Stéphane and Velásquez, Andrés. "CoronApp, Medellín me Cuida and CaliValle Corona go to the lab - or how you can hack CoronApp without even trying to." *Fundación Karisma*. 17 April 2020. <https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/>.

[119] Dludla, Nqobile and Donovan, Kirsten. "Telkom, Samsung team up with South African government to track those with COVID-19." *CNBC Africa*. 4 April 2020. <https://www.cnbcafrica.com/news/2020/04/03/telkom-samsung-team-up-with-south-african-government-to-track-those-with-COVID-19/>.

[120] Moche, Tshepiso. "COVID Tech Part I: Government, UCT partner for tracing app." *SABC News.* 29 April 2020. <https://www.sabcnews.com/sabcnews/COVID-tech-app-developed-to-help-trace-those-infected-by-COVID-19/>.

[121] Chaturvedi, Aditya. "How South Africa uses tech to fight COVID-19." *Geospatial World*. 21 April 2020. <https://www.geospatialworld.net/blogs/how-south-africa-uses-tech-to-fight-COVID-19/>.

[122] "Health Connect for COVID-19." *Praekelt.org*. Accessed 18 March 2020. <https://www.praekelt.org/>.

[123] "Saudi Arabia launches "Tawakkalna" app to issue movement permits." *Saudi Gazette.* 4 May 2020. <https://saudigazette.com.sa/article/592657>.

[124] Naar, Ismaeel. "Saudi Arabia partially lifts coronavirus curfew nationwide, Mecca lockdown remains." *Al Arabiya*. 26 April 2020. < https://english.alarabiya.net/en/coronavirus/2020/04/26/Saudi-Arabia-partially-lifts-coronavirus-curfew-nationwide-lockdown-on-Mecca-remains.html>.

[125] Whittaker, Zack. "A passwordless server run by spyware maker NSO sparks contact-tracing privacy concerns." *Tech Crunch.* 7 May 2020. <https://techcrunch.com/2020/05/07/nso-group-fleming-contact-tracing/>.

[126] Abueish, Tamara. "Coronavirus: Abu Dhabi launches app to track cases, curb outbreak." *Al Arabiya.* 19 April 2020. <https://english.alarabiya.net/en/coronavirus/2020/04/19/Coronavirus-Abu-Dhabi-launches-app-to-track-cases-curb-outbreak.html>.

[127] Nafie, Muhammed. "UAE's coronavirus tracing app – Is it compulsory and other questions answered." *Al Arabiya.* 20 April 2020. <https://english.alarabiya.net/en/coronavirus/2020/04/20/UAE-s-coronavirus-tracing-app-Is-it-compulsory-and-other-questions-answered->.

[128] Ibid.

[129] "Coronavirus treatment system." *Ac19.ir*. Accessed 18 March 2020. <https://ac19.ir/>.

[130] Landau, Noa, Harel, Amos, and Breiner, Josh. "Attorney General Approves Cyber Tech to Track Coronavirus Patients." *Haaretz.* 14 March 2020. < https://www.haaretz.com/israel-news/.premium-israel-to-use-cyber-tech-to-track-coronavirus-patients-1.8675008?=&ts=_1584226332456>.

[131] Ibid.

[132] Gross, Juda Ari. "Government okays mass surveillance of Israelis' phones to curb coronavirus." *The Times of Israel*. 15 March 2020. <https://www.timesofisrael.com/government-okays-mass-surveillance-of-israelis-phones-to-curb-coronavirus/>.

[133] Landau, Noa, Harel, Amos, and Breiner, Josh. "Attorney General Approves Cyber Tech to Track Coronavirus Patients." *Haaretz.* 14 March 2020. <https://www.haaretz.com/israel-news/.premium-israel-to-use-cyber-tech-to-track-coronavirus-patients-1.8675008?=&ts=_1584226332456>.

[134] "P.M. Netanyahu Locks Down Israel Over Passover." *Time.* 6 April 2020. <https://time.com/5816507/israel-benjamin-netanyahu-lockdown-passover-coronavirus/>.

[135] "Coronavirus: Israel halts police phone tracking over privacy concerns." *BBC.* 23 April 2020. <https://www.bbc.com/news/technology-52395886>.

[136] Ibid.

[137] Scheer, Steven and Cohen, Tova. "Israel extends coronavirus cell phone surveillance by three weeks." *Reuters.* 5 May 2020. <https://www.reuters.com/article/us-health-coronavirus-israel>.

[138] Fahim, Kareem, Kim, Min Joo, and Hendrix, Steve. "'I can't be afraid of the risk to privacy right now': Coronavirus and tracking app surveillance." *Independent.* 8 May 2020. <https://www.independent.co.uk/news/long_reads/coronavirus-lockdown-korea-singapore-turkey-surveillance-privacy-tracking-app-a9499526.html>.

[139] "Washington Post-University of Maryland national poll, April 21-26, 2020." *Washington Post.* 5 May 2020. <https://www.washingtonpost.com/context/washington-post-university-of-maryland-national-poll-april-21-26-2020/3583b4e9-66be-4ed6-a457-f6630a550ddf/?itid=lk_inline_manual_3>.

[140] Chazan, David. "French public hostile to proposed COVID-19 contact-tracing app." *The Telegraph.* 12 April 2020. <https://www.telegraph.co.uk/news/2020/04/12/french-public-hostile-proposed-COVID-19-contact-tracing-app/>.