INTERNATIONAL COMPUTATIONAL LAW JOURNAL

CODEX SOURCE ARCHIVE

Ubiquitous Gaze: Privacy Protection in the Era of COVID-19

Adam Au

Computational Law Report · Special Release: COVID-19 · 2020-05-20

Reader edition prepared by The Research University under CC BY 4.0. This cover was added; the original PDF pages follow unchanged. Original authorship, publication identity and source links are preserved. This independent republication is not sponsored or endorsed by Stanford University, Stanford Law School, CodeX or MIT.

Volume 1 · Issue 3 · Emergency Technology, Privacy and Public Trust

Original source and license evidence are recorded on the article landing page.

MIT Computational Law Report

Ubiquitous Gaze: Privacy Protection in the Era of COVID-19

Adam Au

Published on: May 20, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

Introduction

The COVID-19 pandemic has resurfaced age-old discussions about how to appropriately balance public interests and privacy against measured surveillance that leads to better safety and health outcomes. As part of a multi-pronged approach to fight the pandemic, traditional public health authorities rely on a strategy comprised of social distancing, contact tracing, and isolation to reduce the spread of the disease.[1] When there is a confirmed case or when an individual displays symptoms of the virus, teams of investigators identifies the other people that came into contact with that individual and efforts are made to notify and isolate those individuals—these processes broadly make up exposure notification and contact tracing. One challenge with the COVID-19 pandemic is that up to half of transmissions occur from pre-symptomatic individuals.[2] According to recent studies from the University of Oxford, this means that manual contact tracing is not fast enough to slow transmission.[3] This presents a challenge whose solutions have both risks and rewards.

In the era of COVID-19, one of the most accessible and cost-effective ways to collect such information is by using metadata about an individual's interactions and locations, as recorded by their smartphones and mobile networks, to create a digest of the places that person has been and the people they have come into contact with. This technology can be used to conduct more timely, accurate, and efficient contact tracing than the traditional, manual efforts. A model at the University of Oxford projects that mobile phone applications implementing instantaneous contact tracing could help reduce the average number of people infected by each infected person to under 1.0, under the threshold for preventing the virus from spreading further.[4] Countries such as Singapore and South Korea have been relying on digital tools to facilitate contact tracing, including mobile alerts for those infected and public heat maps that show places with high rates of infection.[5]

These concerns, however, are not without cost. Citing the severity of the threat posed by COVID-19, government entities, network providers, and affiliated technology companies have obtained great latitude in deploying sweeping surveillance measures. These measures temporarily reduce individual privacy, represent new opportunities for collective and individual exploitation, and usually favor short-term thinking over long-term thinking. Privacy activists have raised important questions about how governments acquire and use this data, how it is stored, how long these measures will be in place, what oversight mechanisms exist, and how it is otherwise possible to

effectively limit the ability of authorities to abuse these new digital tools after the pandemic is over.

Specific questions in this crisis also examine the actual effectiveness of these apps. While many tech evangelists see this as an opportunity to experiment and deploy the latest and greatest technology, many exposure notification apps generate false positives, placing undue hardship on users of such apps. If data is leaked, patterns of behavior and interaction can be aggregated, exploited, and published for the world to see. For example, there are greater opportunities for people to be blackmailed can be blackmailed if they visit locations that are taboo. Algorithmic redlining and zoning can lead to new forms of discrimination.[6] Then, at a macro level, these gradual erosions of trust will further reduce trust between individuals and the institutions governing them.

This perennial tug-of-war between a need for privacy and active government intervention will persist far beyond this virus. The reality is that even after the danger of COVID-19 subsides, there will be many challenges to the way that people organize and govern themselves. As a practical matter, this means that governing bodies around the world will face challenges for judicial review, regulatory reform, and the passage of new laws and regulations to manage the risk from this and other crises. Yet, understanding this balance of proportionality between exercising executive power, preserving individual privacy rights, preserving collective privacy rights, and achieving epidemiological utility is one fraught with questions and concerns that lack any sort of global consensus. This paper is not an in-depth critique of the proportionality of any specific government's choice of action. Rather, this paper aims to survey that various approaches that combine the use of applications, tools, and legal strategies deployed by several countries around the world combating COVID-19.

Proceeding in two parts, this paper first provides an overview of the different legal and technical efforts carried by a selection of countries or cities to combat the disease. The second part explores the potential legislative, technical, and legal mechanisms to improve these efforts.

Part I: Overview of Legal and Technical Efforts Deployed to Combat COVID-19

South Korea

As the gravity of the pandemic takes hold, South Korea has been aggressive in its efforts to tackle the coronavirus. The process to eliminate the spread of the virus in South Korea has been divided into four stages: (i) investigation, (ii) exposure risk

assessment, (iii) contact classification, and (iv) contact management.[7] During the investigation phase, basic information, including a patient's activity history, is collected by an interview process of the patient, family members and healthcare workers.[8] To the extent supplementary information is required during the risk assessment stage, more granular information such as medical records, cellular GPS data, credit card transaction information, and CCTV footage may be collected.[9] Contacts identified based on the collected information are subject to self-quarantine along with mandatory health education and symptom monitoring.[10]

These measures are being amplified through the use of technological tools. According to the Yonhap News Agency, a government-funded media agency, the Korea Centers for Disease Control and Prevention (KCDC) initially had to request for data such as closed-circuit television (CCTV) footage and credit card transactions of confirmed patients from police investigators.[11] A new data platform co-developed by the Ministry of Science and ICT, the Ministry of Land, Infrastructure and Transport and the KCDC was launched on March 26, 2020 and allows data from confirmed patients to be provided to health investigators and analyzed proactively.[12] The Korean National Police Agency, the Credit Finance Association, South Korea's three mobile carriers, and 22 credit card issuers are working together to provide data and other insights.[13] The platform is based on a smart city data hub program developed by the central government and the municipal government of Daegu. [14] [15] As a tool for big data analysis, the platform produces insights for cities that want to launch new smart services using data related to traffic, energy use, environmental quality, and safety.

With these digital tools in place, health officials are able to correlate interview results with patient location maps via data uploaded to this platform, developing a comprehensive overview of who has been infected and where they have been. Moreover, this type of big data analysis provides officials with real-time data feeds on confirmed patients, including their whereabouts and the time spent at each location.[16] Armed with this information, the platform can facilitate the epidemiological evaluation of cases by looking at different clusters and disclosing the source of transmission. Contrasted against traditional measures used in the past, these new methods do not require numerous exchanges of documents and phone conversations among South Korea's 28 relevant agencies.[17] The government has claimed that this platform can enhance the accuracy and efficiency of contact tracing by reducing the lead time for identifying cases from 24 hours to less than ten minutes.[18] A reduced workload of

health officials can also ensure quicker government response to avoid further spread of the disease.[19]

In addition to monitoring the spread of the disease, applications have been developed for those who have received a positive infection. Anyone who has come into contact with a confirmed carrier is subject to a mandatory, two-week, self-quarantine.[20] Once self-quarantine subjects receive an order from their local medical center, they are legally prohibited from leaving their quarantine areas and are instructed to maintain strict separation from other people including their family members.[21] Those in lockdown are assigned to a local government official, who is authorized to track the development of any symptoms, and mobile testing teams are deployed to collect samples if the situation worsens.[22] [23]

Technology is used to aid these traditional processes by the application "Self-Quarantine Safety Protection," (see Fig.1), which was developed by the Ministry of the Interior and Safety and allows those who have been ordered not to leave home to stay in contact with caseworkers and report on their progress.[24] Self-Quarantine Safety Protection also uses GPS to keep track of the location of confirmed patients to ensure they are not breaking their quarantine.[25]

Other tools in the South Korea ecosystem include those meant to aid those in the public seeking to avoid contact with COVID-19, among them are the "Corona 100m" application, which alerts users when they come within 100 meters of a location visited by an infected person,[26] the Coronamap, which is a website that shows the travel histories of confirmed COVID-19 patients,[27] and Coronaita, which aims to function like a search engine for information on coronavirus-hit areas.[28]


오후 6:35
자가격리자 안전보호
자가진단 하기
마지막 자가진단 없음
자가진단 목록
정보 등록/수정
생활수칙안내
전담공무원 연락처
1339
Ver 1.1.6

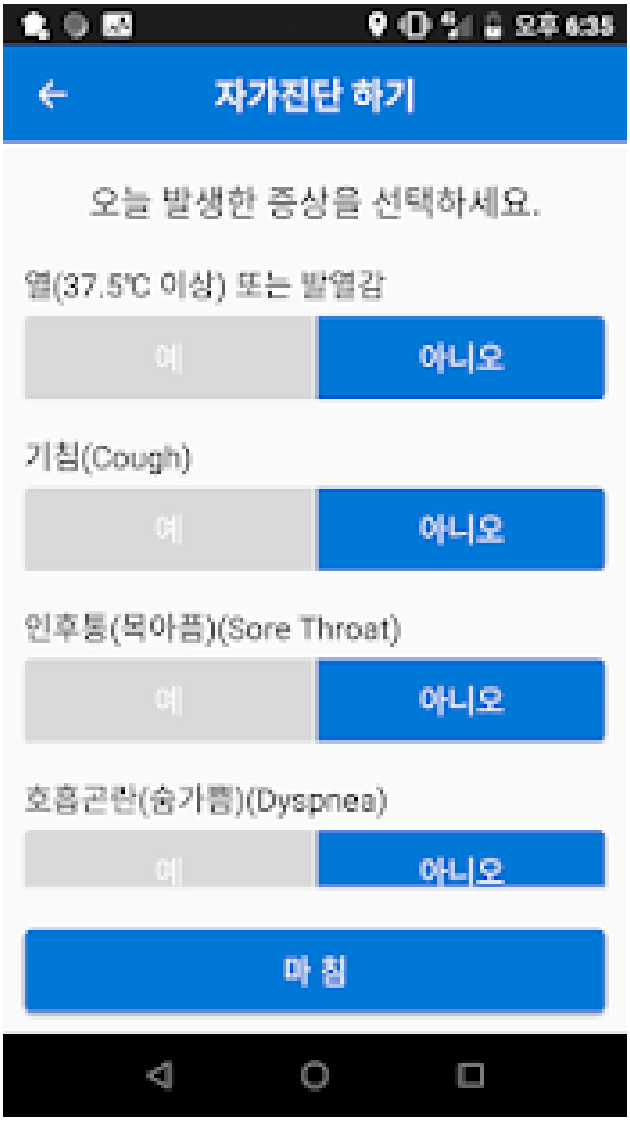


Fig.1 User Interface of Self-Quarantine Safety Protection. From Google Play website. https://play.google.com/store/apps/details?id=kr.go.safekorea.sqsm

These measures, however, are not without a cost. During South Korea's fight against the virus, digital footprint of all citizens are visible to the government, part of the private sector, and, in some cases even some members of the public. For example, when a person tests positive, the city or district he/she inhabits might send out an alert to people living nearby about the movements he/she made prior to being diagnosed.[29] An alert can contain the infected person's age and gender, as well as a detailed log of their movements down to the minute.[30] Other countries, including Singapore, release data such as the age or gender of confirmed patients, but nothing as detailed as in

South Korea. In some districts, disclosure of public information includes which rooms of a building the person was in, when they visited a toilet and whether they wore a mask.[31] Even overnight stays at love motels are reported to have been noted.[3233] It is reported that on April 7, 2020, as a measure to reduce any flouting of mandatory quarantine orders, the South Korean government proposed to impose self-isolation electronic wristbands on confirmed patients. The suggestion was opposed by the Ministry of Health and Welfare due to the potential human rights violation.[34] Beyond the short term impact, however, many long term repercussions remain unknown. However, it is likely that the perception of individual privacy within South Korea will be forever minimized.

Underwriting the large-scale government effort and high-level openness to mobilize resources is an established legal apparatus that sets a limit on the duration of the data usage. Under Article 76-2(4) of the South Korea's Infectious Disease Control and Prevention Act (IDCPA), the information collected will be destroyed when the "relevant tasks have been completed."[35] The South Korea government further clarified that the data collection efforts will end when the coronavirus outbreak is over and that all personal data might be deleted.[36] Despite the extensiveness of surveillance and data sharing, the Korean public broadly supports the government publishing individuals' movement argued Youngkee Ju, a researcher in health journalism at Hallym University in Chuncheon.[37] In a 1,000-person survey published in February and March, most respondents supported the government sharing travel details of people with infectious details and preferred the additional safeguard for public good over individual privacy rights.[38]

Hong Kong

Hong Kong was one of the first cities in the world paralyzed by the virus. After a brief period of recording low case numbers, Hong Kong was hit by a second wave of outbreak in late March.[39] As residents returned to the country from work trips, study abroad programs, or to seek safety after outbreaks in other cities around the globe, many inadvertently brought the virus back with them. This migration threatened to drive up the rate of infection which had at least been somewhat under control.[40] As a result, the Hong Kong government implemented a series of additional, stringent restrictions including a mandatory 14-day quarantine for inbound travelers.[41]

Like South Korea, Hong Kong has looked to the use of technological tools as a way to boost the abilities of their constituents. Ensuring the efficacy of traditional quarantine

efforts requires a great degree of human interaction in order to maintain compliance with a quarantine order. Many of these analog solutions are difficult to implement, costly, and might risk the health of those staying in close proximity to one another. Hong Kong's efforts have been furthered by the work of a team of researchers and engineers, led by Professor Gary Chan of the Department of the Computer Science and Engineering and Director of Entrepreneurship Center at The Hong Kong University of Science and Technology. This team led the design of an automated geofencing technology called "Signature Home,"[42] which has been used to develop a mobile application called "StayHomeSafe."[43] (See Fig. 2 & 3)

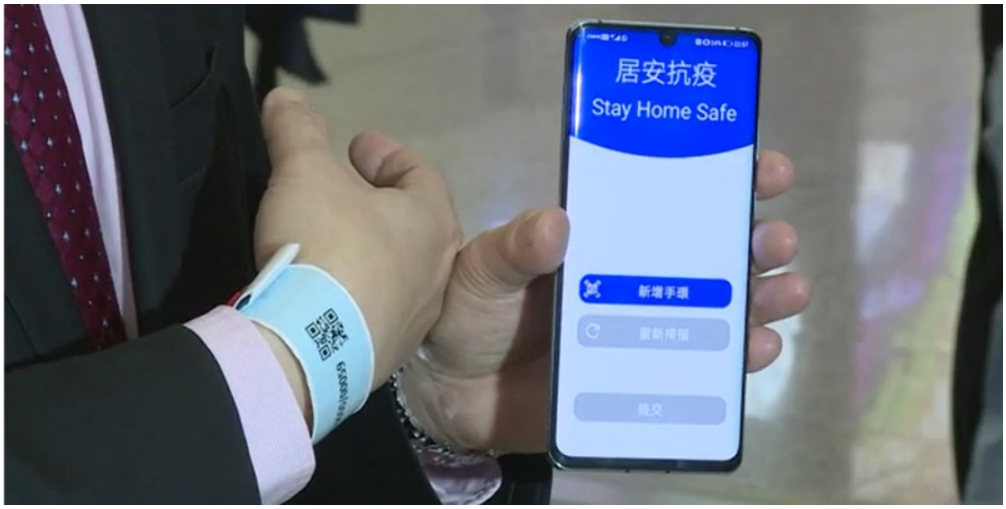


Fig.2 The use of a mobile app StayHomeSafe paired with a Bluetooth-enabled wristband. From the Register website, British technology news and opinion website. https://www.theregister.co.uk/2020/03/19/hong_kong_wearable_trackers_mandatory/


1:43
居安抗疫
Stay Home
Safe
ADD WRISTBAND
RE-SCAN
SUBMIT



Fig.3 User Interface of the StayHomeSafe Application on Google Play. From the Google Play website. https://play.google.com/store/apps/details?id=com.compathnion.equarantine&hl=en

The app has been used by the public since March 14, 2020 as a way to monitor people under home quarantine.[44] Paired with an electronic Bluetooth wristband, the app can detect whether the detainee is complying with the requisite quarantine order and alert the relevant authorities about non-compliance.[45]

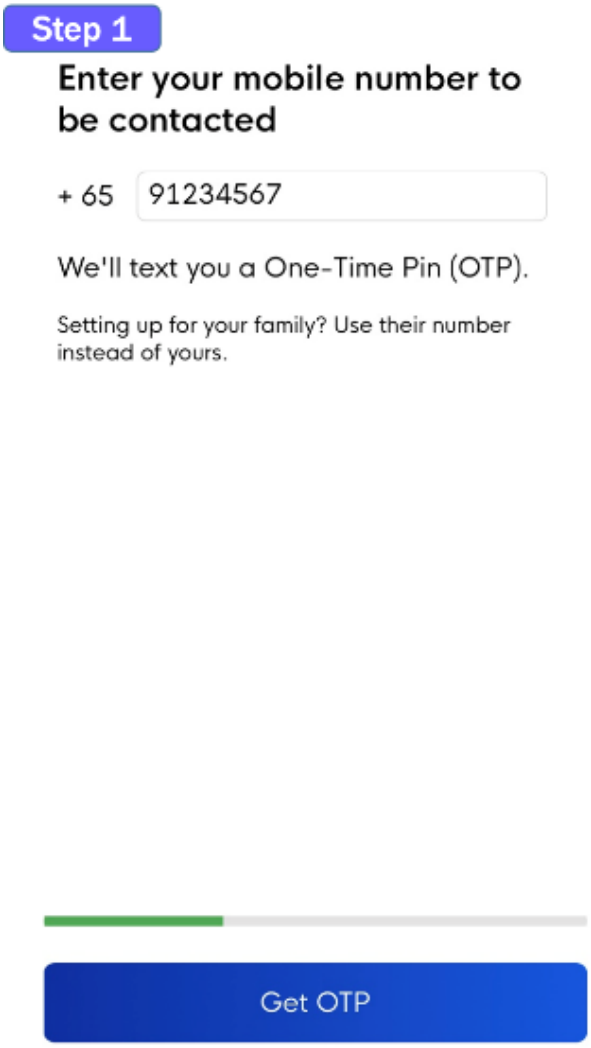
The key idea of the Signature Home geofencing technology is that the collective signal variations within a certain location are unique to that location, forming a sort of multi-factor "signature" for each user.[46] The technology collects data from various connections made by the user, including environmental signals such as Wi-Fi and Bluetooth in the dwelling place as its signature.[47] If a newly collected signal variation deviates from the signature, it is likely that the person has left the designated location in breach of the mandatory quarantine rules.[48] By continuously collecting and

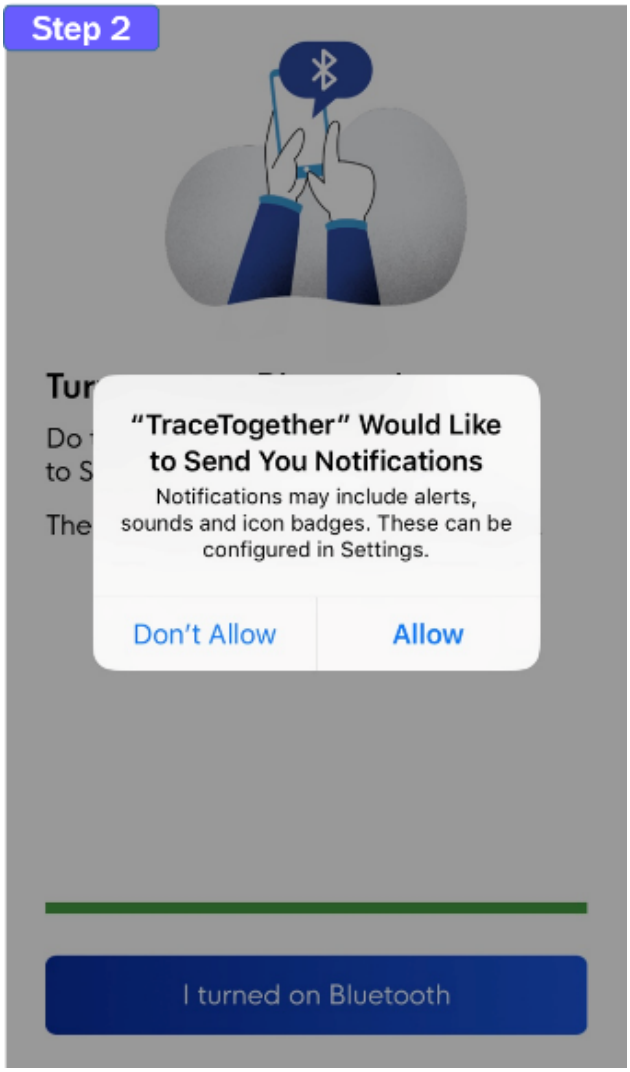
understanding the change of the composition of signals collected in a place, aided by machine learning and data analytics techniques, Signature Home manages to adapt to changes to the home environment to ensure more accurate monitoring.[49] As with other machine learning and data analytics technologies, there is a risk of false-positives, especially early on as data is being trained. Many of these technologies will need to be fine-tuned over time and limited in scope to specific use cases where repetition is easily identifiable.

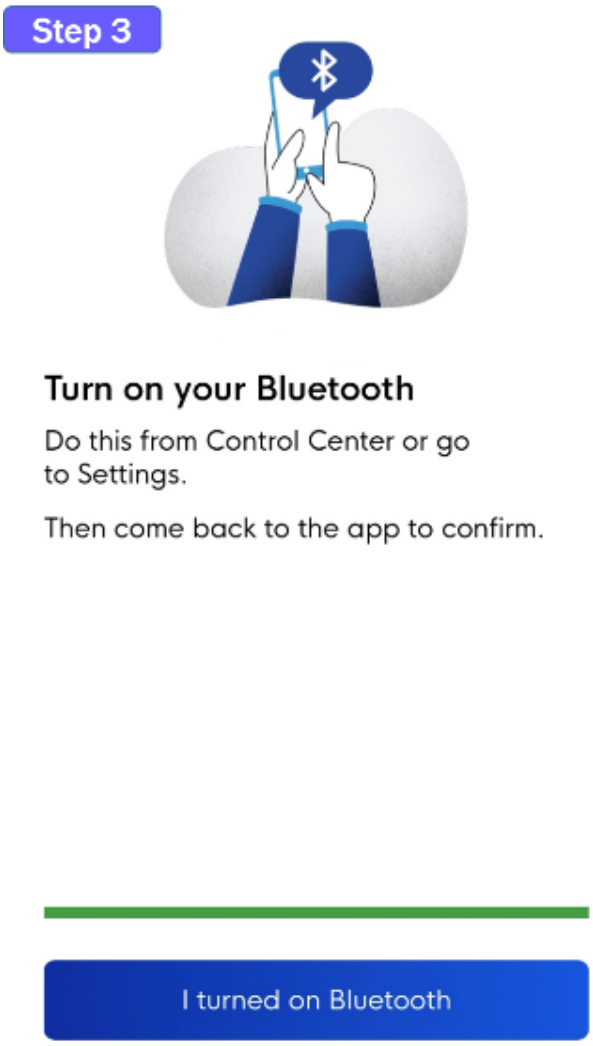
Stepping up the monitoring effort, short message service (SMS) instructions on activating the "StayHomeSafe" mobile app have been sent to all inbound travelers arriving in Hong Kong since March 20, 2020.[50] In less than a day, over 7,400 new monitoring wristbands were distributed to people arriving in Hong Kong by air in conjunction with the "StayHomeSafe" mobile app.[51] Armed with this new technology, Hong Kong managed to flatten the second curve of infections without resorting to the kind of complete lockdowns that are paralyzing economies elsewhere. As of May 5, 2020, the city reported no new community infections for over a period of 15-days.[52] Since then, the city has started to ease restrictions and cautiously reopen its economy.[53]

Singapore

The primary focus of Singapore, in combating the spread of COVID-19, has been on contact tracing. The small, island nation has developed a contact-tracing application, "TraceTogether"[54] (See Fig. 4), which can can identify people who have been in close proximity – within 2 meters for at least 30 minutes – to identified coronavirus patients, according to its developers, the Government Technology Agency (GovTech) and the Ministry of Health (MOH).[55] [56] While use of the app is not compulsory, those who use it must enable Bluetooth in their smart phones to allow tracing.[57] Users also need to enable push notifications and location permissions in the app. The app uses encrypted short-distance Bluetooth signals that are exchanged between phones to detect other users in close proximity.[58] Official contact tracers will provide a code that users can match with a corresponding verification code on their app.[59] When requested by MOH, users can send their TraceTogether logs to facilitate the contact tracing process.[60] Up to that point, the authorities, including the MOH and GovTech, have no knowledge of the users' TraceTogether data.[61] [62]


Step 1
Enter your mobile number to be contacted
+ 65
91234567
We'll text you a One-Time Pin (OTP).
Setting up for your family? Use their number instead of yours.
Get OTP


Step 2
"TraceTogether" Would Like to Send You Notifications
Notifications may include alerts, sounds and icon badges. These can be configured in Settings.
Don't Allow
Allow
I turned on Bluetooth


Step 3
Turn on your Bluetooth
Do this from Control Center or go to Settings.
Then come back to the app to confirm.
I turned on Bluetooth

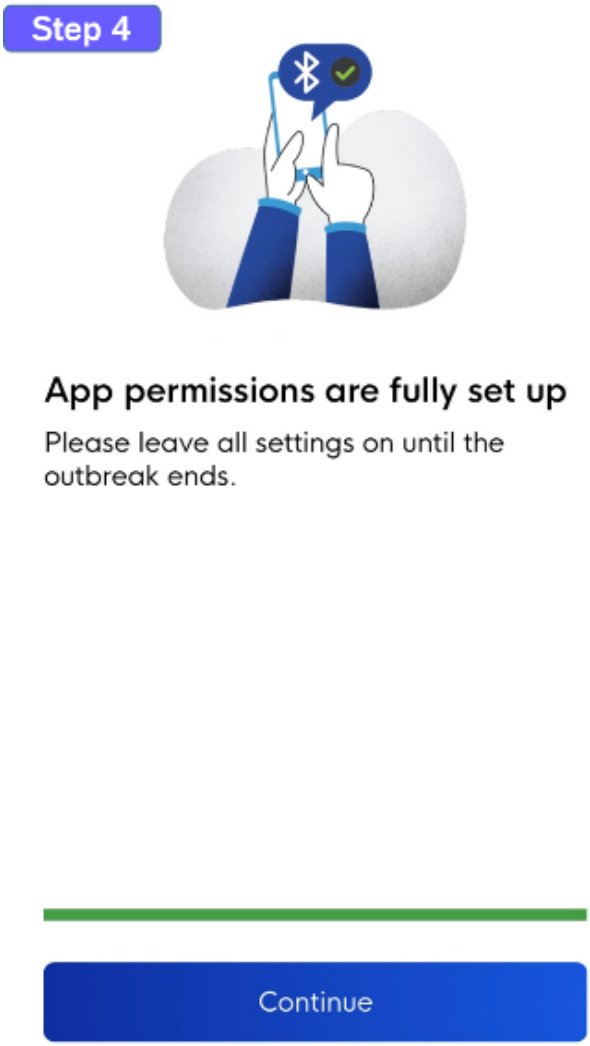


Fig 4. The user interface of the TraceTogether app. Created by SGUnited, GovTech, and the Ministry of Health of the Government of Singapore. From the Government of Singapore website. https://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether

The government claims that the app only records who they might have been close to and that it does not record location data or access the phone user's contact list. Data logs are stored on phones in encrypted form for only 21 days.[63] The data that is collected by the government through this app is the user's mobile number, so that the MOH can contact users quickly if they were in close proximity with an infected case, allowing for easier identification of potential cases and helping to curb the spread of

the coronavirus. When contacted by contact tracers, users will be asked to share their data logs. If they refuse, they can be prosecuted under the Infectious Diseases Act (IDA) and any regulations promulgated thereunder.[64] Further, health officers appointed under Section 55A of the IDA have the power to require any person to furnish any information within his/her knowledge or to produce any book, document or other record, to investigate any suspected outbreak or prevent the possible spread of an infectious disease.[65]

On the downloading sites for Android users[66] and iOS users,[67] TraceTogether expressly states that its functionality will be suspended after the pandemic subsides. While many of the challenges facing other contact tracing apps will be faced by TraceTogether, exploiting the technological apparatus remains at the forefront of the Singaporean government to help reduce the impact of the virus.[68] Recently, the National Parks Board and the Smart Nation and Digital Government Group of Singapore conducted a pilot trial of a four-legged robot called SPOT to assist safe distancing efforts at parks, gardens and nature reserves at local parks.[69] The cameras fitted on SPOT will not be able to track and/or recognize specific individuals, and no personal data will be collected.[70]

China

In China, cases of COVID-19 have reportedly declined at a steady rate since peaking in mid-February 2020, which is at least partially attributable to more draconian measures that the government enacted in order to contain the spread of virus. While some of these measures would be deemed controversial in democratic societies, the combination of technologies, including apps for tracking individuals and pervasive use of CCTV cameras, and in-person enforcement efforts by the Communist Party demonstrates one way strong, top-down governance, early quarantine, and early treatment aided by technology can be deployed to reduce the global spread of the COVID-19.

In Guangzhou, the capital and most populous city of the Guangdong province in southern China, big data technology has been used to track locations and connections, screen priority cases, and effectively forecast the development of the pandemic in real time.[71] By mid-February 2020, Guangzhou managed to track and diagnose 10.18 million people in the community and located 377 individuals with fever and other related COVID-19 symptoms.[72] According to The Paper, a state-funded Chinese media site, the government confirmed that a restaurant owner and his son in Wenzhou, a city

in China's Zhejiang province, were infected and tracked their location and activities for fifteen consecutive days.[73] Supported by mobile data made available to the government by three major local mobile operators, more than 3,615 people who passed by the restaurant during this period were located and notified through SMS.[74] With the aid of technology, a total of 40 people who had visited the restaurant have been identified and were required to get tested in order to decrease the spread of COVID-19.[75]

As the pandemic spreads throughout the country, many see big data tracking as one of the most accessible ways to stop the spread of COVID-19. The Ministry of Industry and Information Technology of the People's Republic of China launched a new service allowing Chinese telecom subscribers to receive a list of provinces and cities visited within the last fourteen (14) days via SMS. The country's three state-owned mobile service providers – China Mobile, China Telecom and China Unicom – started sending SMS to users asking for authorization to access their location data.[76]

Perhaps the most omnipresent surveillance tool China has introduced is the use of a "health code" classification system called the Alipay Health Code. According to Xinhua Press Agency, the official state-run media agency in China, Alipay Health Code was first introduced in the eastern city of Hangzhou on February 11, 2020.[77] This project was completed by the local government with the help of Ant Financial, an affiliate of the e-commerce giant Alibaba, and its online payment platform, Alipay.[78]

After the users add their personal details in the system, Alipay Health Code (see Fig. 5) generates a QR code in one of three colors.[79] A green code enables its holder to move freely without restriction, a yellow code means that the person may be asked to stay home for seven days, and a red code means that the person is subject to a mandatory 14-day quarantine.[80] To change from red to green, a detainee would need to show improved health status on a regular basis. Alipay Heath Code has become an integral part of the authorities' management of people's movement into and out of the affected areas.[81] In Wuhan, the city where the virus was first reported, only those with a green code can take public transportation.[82] As of March 31, 2020, this system is already in use in 200 cities and has been rolled out nationwide.[83]


ShangHai QR Code
GREEN
ShangHai QR Code
YELLOW
ShangHai QR Code
RED

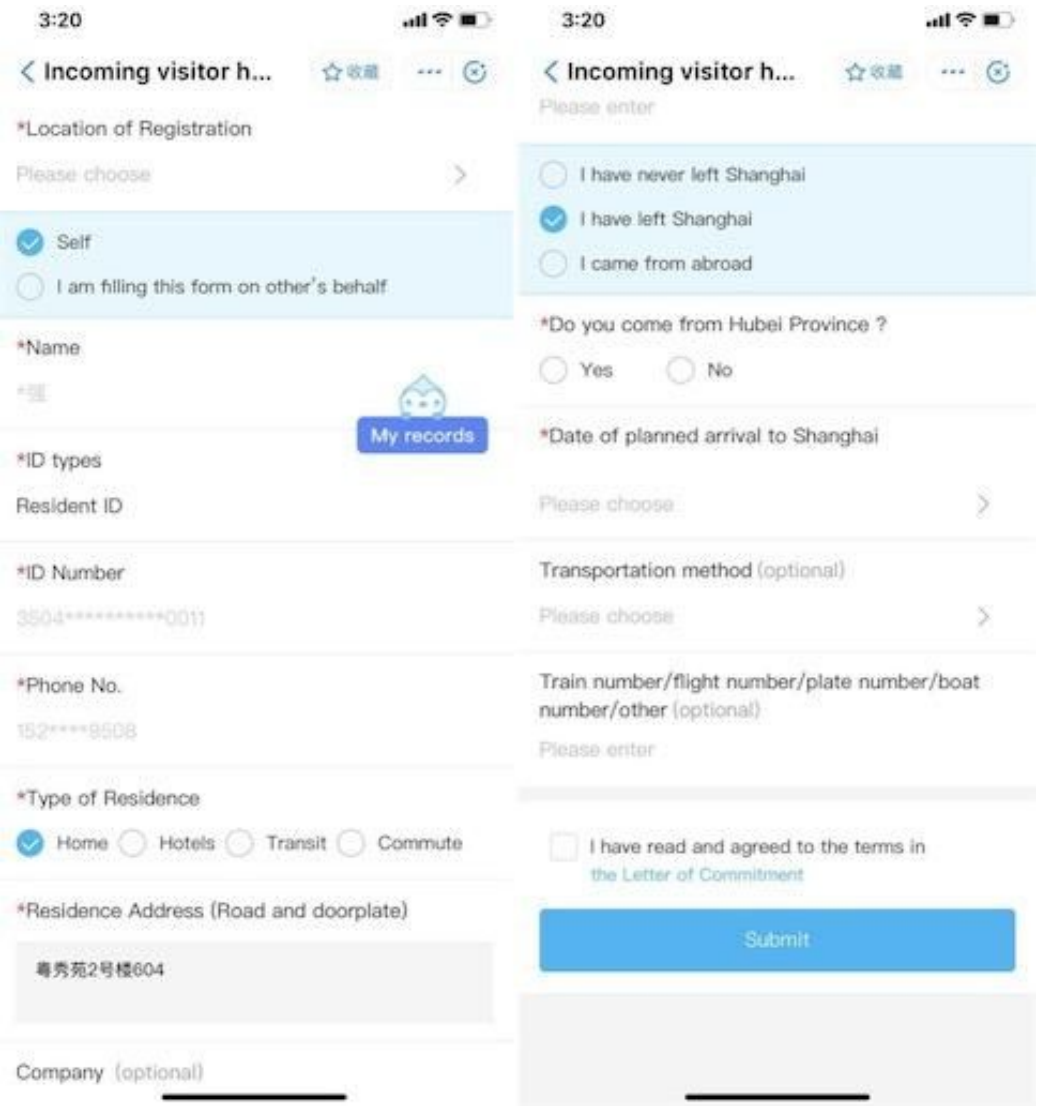


Fig.5 The interface of the Health Code by Alipay. From Eastday website, a shanghai-based news portal. http://english.eastday.com/Latest/u1ai8666477.htm

It was reported that Ant Financial does not provide or operate the service and has no access to the data amassed on its platform.[84] The software was designed solely in support of the Hangzhou city government.[85] Similarly, WeChat, a messaging app owned by tech giant Tencent with over a billion monthly users, worked with authorities to build its own health code system.[86] It collects basic identity and address details as well as a history of close contact with suspected patients, history of travel and history of residence.[87] The app draws on medical information including symptoms, medical treatment, isolated observation, contact information, travel history of the epidemic

area, and the user's travel history including the mode of travel and what seat they sat in, as well as details on the vehicle and its driver.[88] Currently, neither Ant Financial, WeChat, nor Chinese officials have explained in detail how the system classifies people in the country. These platforms have caused great confusion among citizens in China and false classifications examples abound.[89]

China has long had a history of using big events to implement surveillance measures that outlive their original intended purpose; examples of this include the 2008 Beijing Olympics and the 2010 World Expo Show in Shanghai.[90] The continued dissemination of personal data to authorities blurs the already thin line between Chinese tech companies and the Chinese government and continues a general trend toward something resembling a social credit score. According to the New York Times analysis, as soon as a user grants the Alipay software access to personal data, a piece of the program labeled "reportInfoAndLocationToPolice" sends the person's location, city name and an identifying code number to a server.[91] The software does not make clear to its users this connection to the police. However, according to Xinhua Press Agency[92] and an official police social media account,[93] law enforcement authorities were privy to the system's development. The most striking aspect of all was the overt passage of private citizens' data through a one-way, government-controlled valve, a practice that had previously been inferred rather than direct. If nothing else, this absolute collaboration between government and the private sector can serve to indicate what the tradeoffs between privacy and utility might be. The continued compliance of data-driven technology companies operating in China under the mandate of a powerful one-party state will remain deeply impressed in the fabric of mainstream operation execution and the long-term effects of this collaboration remain to be seen.

United States

Like China, Singapore, and South Korea, the United States has been similarly impacted by COVID-19 and have taken a more privacy preserving approach to combatting the pandemic. As of May 9, 2020, the United States remained the country with the highest number of confirmed cases of COVID-19.[94] According to the Guidance Regarding Methods for De-identification of Protected Health Information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the U.S. Department of Health and Human Services has strict rules on the disclosure of cases in each city, as well as according to age, race, and geographic

region of residence.[9596] So far, the statistics of confirmed patients released by the US governments at all levels have been limited to counties, not specific cities.[97]

The same legal levers in Asia that enable widespread surveillance measures have no comparable analogue in the United States. This difference can be best explained by an advocacy of privacy and civil liberties protection – a value that is deeply entrenched in the American constitutional spirit, as well as it being a deep-seated construct of the collective American identity. As a result, data sharing American researchers often lack the availability of data to more granular analyze and forecast the spread of COVID-19, unlike governments in other countries who are harnessing a wealth of information from their more centralized medical systems.[98] Critics of the limited public reporting have argued that this lack of data prevents the country from effectively curbing the spread of the virus.[99]

The United States' broad, federalist approach contrasts sharply with that of the small, more centralized one employed by Singapore, which has fought the virus effectively by publishing anonymized data about suspected linkages of cases.[100] The Singaporean authorities sometimes list neighborhoods where the patients lived, as well as their workplaces and the churches or mosques that they attended.[101] Moritz Kraemer, a leading researcher at Oxford University whose research team is mapping the global spread of the coronavirus, argued that there was wide demand for data on the disease across the scientific community and that it needed to be tabulated to facilitate detailed analysis.[102] His research was aided by the breadth of the data collected in countries such as China, which includes, among others variables, a patient's age, sex, travel history and history of chronic disease, where the case was reported, and the dates of onset of symptoms, hospitalization and confirmation of infection.[103]

The United States consists of a mix of federal and state laws on privacy. Some federal statutes address specific sectors, such as financial services or healthcare, whereas state-level legislation addresses a wide range of other issues and often differs from state to state. This segmented approach and the lack of a federal privacy regulation, however, has led to inconsistent data collection and a more opaque understanding of cases throughout the United States, as well as burdens on the local and states governments that are tasked with piecing together a solution comprised of divergent methodologies.[104] Often, there is a breakdown between what data states collect, what data cities collect, and what data counties collect. For example, Connecticut lists data by town.[105] Florida provides its residents with extensive data on the cities affected,

the number of people tested, the age brackets of patients, whether they are Florida residents, and the number of cases in nursing homes.[106][107] Health departments in the Bay Area have made a case against detailed disclosure of information due to concerns that releasing more granular data will lead to heightened discrimination against certain Asian communities in which clusters of COVID-19 may occur.[108] And while all of this information can be aggregated in dashboards created by others, like the John Hopkins University dashboard for United States cases by county, it remains to be seen whether a more centralized system could have reduced the spread more effectively and what long term impacts this might have on the economy, the trust of the citizens, and the downstream health consequences.[109]

European Union

By comparison, the European Commission (EC), in the face of an avalanche of confirmed COVID-19 cases, has kick-started a discussion with mobile phone operators about the provision of aggregated and anonymized mobile phone location data.[110] The plan is to analyze mobility patterns including the effects of confinement (and de-confinement) and social distancing measures, and thereby assess the risk of contagion. This would be an important and arguably more proportionate input for tools that are modeling the spread of the virus and would allow the EC to assess the efficacy of the measures that have been taken to contain the pandemic.[111] [112]

In the same regard, EU telecommunication companies have been sharing aggregate data with various agencies to develop new application. For example, Orange in France is sharing aggregated and anonymized mobile phone geolocation data with Inserm, a local health-focused research institute, to enable them to anticipate and manage the spread of the pandemic more effectively.[113] The research focused on examining the spontaneous changes in mobility occurring before and during the lockdown, and their impact on the evolution of the pandemic. The data will be integrated into models of pandemic spread developed by the research team, which would improve predictions of the spread of the virus and identify regions at risk of becoming clusters and of having their healthcare systems overwhelmed.[114]

Part II: Limiting the Unintended Consequences of Surveillance

There is no doubt that the development of digital technology holds the promise of great benefits to humankind. The migration from analogue to the digital world is

continuing at a rapid pace. Humans are awash in data. However, data is often misinterpreted or overused without adequate safeguards.

Amidst imposed lockdowns and restrictions on freedom of movement, law enforcement agencies are finding themselves playing a critical role in halting the spread of the virus while also preserving public safety and social order. As a result, human rights, civil liberties, and fundamental principles of law may be compromised if the government does not navigate these challenges carefully. The remainder of this section fleshes out some general strategies that should be considered, based on the preceding analysis, when implementing law and computational solutions together.

Legislative Oversight

One option to reduce the potential for abuse is to build cohesion at the legislative level. The European Data Protection Board (EDPB) of the EU issued a statement on March 16, 2020 giving a clear framework for the processing of personal data under the General Data Protection Regulation (GDPR) during the pandemic.[115] The GDPR provides rules to govern the application of processing personal data in the current context of COVID-19, laying out the legal grounds for employers and competent public health authorities to process personal data in the context of pandemics without the need to obtain the consent of data subjects.

For the processing of electronic communication data such as mobile location data, additional rules apply. The ePrivacy Directive stipulates that location data can only be used by the operator when they are made anonymous or with the consent of the individuals. Public authorities of member states should aim to process location data in an anonymous way by aggregating data in such a way that it cannot be reversed to personal data.[116] A member state is obligated to put into place adequate safeguards, such as the right to judicial remedy.[117] It is important to note that, according to the EC, the data collected will only be kept as long as the crisis is ongoing, and the collection will be fully in compliance with the ePrivacy Directive and the GDPR.[118]

On March 21, Frankfurter Allgemeine Zeitung, a German newspaper, reported that the German health ministry had drafted changes to a law called the Infection Protection Act that allow, among other things, the tracking of people who were in contact with those infected with the coronavirus.[119] This act carefully sets a legal boundary for regulating the use of personal privacy data and avoiding the legal risks of unauthorized use.

In South Korea, the prevailing public health law provides the government with an adapted legal apparatus to activate collective effort to combat the disease. The law itself is the upshot of the painful lesson learned in the 2015 Middle East respiratory syndrome outbreak, which saw the South Korean authorities struggling to reduce the gravity of the infection after a delayed initial response. The epidemic built social consensus on the importance of data collection and use in epidemic response and prompted amendment of the IDCPA.[120] [121] Under the revised Act, health officials can have access to the patients' personal information in exceptional cases like containment of infectious disease. Article 76-2(1) of the IDCPA enables the KCDC to require medical institutions, pharmacies, corporations, organizations, and individuals to provide information concerning patients and persons feared to be infected. [122] This is augmented by Articles 76-2(2) which equips the Minister of Health and Welfare with extensive power to collect private data from confirmed and potential patients in absence of a warrant from private telecommunications companies and the police agency. Such comprehensive legislative provisions empower authorities to extract surveillance footage, credit card histories and geolocation data of both confirmed and potential patients. This explains, in part, how the South Korean government has been able to rapidly contact-trace its citizens to limit the spread of the virus outbreak.[123]

In Singapore, the Personal Data Protection Commission issued guidelines clarifying that the coronavirus falls under the emergency exception under the Personal Data Protection Act (PDPA), such that personal data may be collected, used or disclosed without consent for purposes of safeguarding the health of the occupants and contact tracing and other response measures. The collected personal data must continue to comply with all other data protection obligations under the PDPA such as, amongst others, the obligation to protect personal data by making reasonable security arrangements to prevent unauthorized access, collection, use and disclosure, and the obligation to cease retaining such personal data as soon as it is reasonable to assume that the original purpose is no longer being served and retention is necessary for legal or business purposes. [124] [125]

The Hong Kong Privacy Commissioner clarified that "there are sufficient legal and justifiable bases" on which the government may collect and use information obtainable offline or online with the aid of devices, applications, software or supercomputers with a view to tracking potential COVID-19 carriers or patients in the interests of both the individuals concerned and the public.[126]

In the absence of a more robust ePrivacy Regulation, the EU will continue to fall back on the old regime of the ePrivacy Directive, leading to potential mismatch and confusion among member states on the continued applicability and practical relevance of the ePrivacy Directive.[127]

Similarly, in the United States, there is a call to revisit HIPAA regulations in order to enlarge the scope of legislative permission and counteract the destruction of the virus during the current global emergency. HIPAA was designed for the protection of personal data at doctors' offices and in hospitals and includes provisions for the release of otherwise protected information during emergencies. Many experts, including Glenn Cohen, a bioethics expert at Harvard Law School, have argued that the guiding principle during this crisis should be "sharing more rather than less."[128] Regardless of the merits of these claims, the coronavirus pandemic will likely to spur a careful reassessment of medical privacy laws in the United States for years to come.

Data Anonymization and Protection

Another way that communities around the world can improve privacy outcomes while leveraging the utility of the information itself is through data anonymization and protection. Personal information, especially information that has not been anonymized, must be properly secured and encrypted and access to it must be carefully managed. In the realm of the EU, the GDPR specifically requires measures to implement appropriate data protection principles and safeguard individual rights during the processing activities and business practices from the design stage and throughout the lifecycle.[129] [130] GDPR further requires systems that are designed to process personal data to ensure data minimization by default, while incorporating all other GDPR obligations into the design of the system.[131] [132] This option provides governments with the ability to track the movement of their citizens while minimizing the ability of the apps to infringe upon data privacy rights. In the United States, a team led by MIT computer scientist Ramesh Raskar, has released a prototype application, "Private Kit: Safe Paths."[133] Users can provide information about themselves on the app and declare if they are infected or not.[134] Their location and movements are logged, stored on the phone in encrypted form and shared with third parties only with prior consent.[135] Users can choose to receive notifications if they have been near a confirmed patient, but the app will not divulge the name or identity of individuals, unlike more authoritarian, government-led solutions.[136]

In South Korea, to protect the information gathered, access to the platform and the level of access will be differentiated according to the duties of the authorities in charge. Under the current arrangement, KCDC officials and local government officials in charge of contact tracing need to have the necessary security clearance to access the collected data. Further, the new data platform designed for virus outbreak runs on a private network to shield the system from hacking and adopts security technologies like double firewalls as well as the thorough log-in management system to avoid abuse of personal information. While in operation, the platform will be constantly monitored by computer security experts and the technology will be constantly updated based on the changing pandemic outlook.[137]

On the other hand, in most European countries, the use of individual smartphone location data to track the spread of the pandemic would violate national and EU privacy laws. In Berlin, the Fraunhofer Heinrich Hertz Institute is developing an application that anonymously stores information on the proximity and duration of interpersonal connections on a mobile phone for up to two weeks. The application does not use any location data or personal data and the data collected can help the public health department to reconstruct the infection pattern digitally without exposing personally identifiable information.[138] [139]

While these restrictions are acceptable in principle, current technologies might not be able to offer impermeable protection of individual identities. In its letter to the EC, the EDPS emphasized the importance of effective data anonymization using techniques that genuinely block the re-identification of data.[140] [141] [142] Researchers have often demonstrated that anonymized data can easily be reidentified; for example, location data typically includes many easily identified individual tells, such as home address.[143] A research study conducted by Imperial College London and Belgium's Université Catholique de Louvain found that 99.98% of Americans could be correctly re-identified in any dataset using 15 demographic attributes.[144] Their results suggest that even heavily sampled anonymized datasets are unlikely to satisfy the modern standards for anonymization set forth by GDPR and provide a serious challenge to the technical and legal adequacy of the de-identification "release-and-forget" model.[145] According to the EDPS, effective anonymization requires more than removing obvious identifiers such as phone numbers and International Mobile Equipment Identity numbers; aggregated data can provide an additional safeguard.[146] [147]

Purpose and Time Limitations

A third strategy that can be used to ensure these apps do not outlive their original motivation is to set purpose and time limitations. Personal data that is collected and processed to track the spread of the coronavirus should not be used for any other purpose. According to the GDPR, national authorities should seek to ensure that personal and medical data are exclusively used for public health reasons.[148] In South Korea, the scope of data collected is claimed to be kept to a minimum and a due procedure is imposed on the officials in acquiring the data.[149] For example, an epidemiological surveyor should decide whether additional collection of personal information is needed. If the answer is in affirmative, the official should seek approval from relevant authorities to get access to the data. As for the location information, separate permission from the National Police Agency is required.[150]

Nevertheless, when the pandemic subsides, national authorities will need to scale back their expedient monitoring capabilities. As Yuval Noah Harari, an Israeli historian and a professor in the Department of History at the Hebrew University of Jerusalem, observed in a recent article, "temporary measures have a nasty habit of outlasting emergencies, especially as there is always a new emergency lurking on the horizon."[151] Government authorities must reassure their citizens that these exceptional capabilities will not become the new norm.[152] This deep concern for privacy was echoed by the Office of the United Nations High Commissioner for Human Rights. In a public statement on March 19, 2020, the monitors of freedom of expression and freedom of the media for the United Nations, the Inter-American Commission for Human Rights and the Representative on Freedom of the Media of the Organization for Security and Co-operation in Europe issued a joint statement about protecting the free flow of information during the pandemic, while stressing that "while we understand and support the need for active efforts to confront the pandemic, it is also crucial that such tools be limited in use, both in terms of purpose and time, and that individual rights to privacy, non-discrimination, the protection of journalistic sources and other freedoms be rigorously protected."[153]

Conclusion

In times of conflict and crisis, the argument for executive expediency is frequently voiced as an efficient way to solve the problem. Each case demands a high degree of critical examinations of the broader context and of the applications themselves. Arthur L. Caplan, a bioethics expert at the N.Y.U. School of Medicine, has argued that using

law to justify the limited release of aggregate data is counterproductive to the preservation of public safety.[154] Only with transparent and comprehensive aggregation of available data can law enforcement agencies, health authorities, and security professionals tasked with protecting the public from harm maximize the efficacy of their unusual measures. Further, it is expected that the private sector, at least in some Asian countries, will continue to surrender to the government necessary information about their users, whether driven by their own social responsibility or as a result of unorthodox governmental sequestration.

There is a role for privacy and a role for technology. Governments, citizens, and industry must work together to achieve the most appropriate balance between these two based on their unique circumstances. However, any juxtaposition between disparate measures undertaken by democratic and authoritarian government in time of a global emergency often overlooks the nuanced menu of legislative and executive prerogatives available to each individual regime. It is therefore important to remember that mandatory data collection and dissemination without explicit authorization and absent clear restrictions on data collection method, time, use and purpose may lead to abuses of digital capabilities and infringements on human rights. Should we anticipate a new wave of judicial reviews on the purportedly excessive use of executive power? Will the zealous mining of personal data ultimately be repulsed by public concerns beyond the COVID-19 crisis? Then, there is an issue on contract. If there are contracts in place between the government and third-party companies that are supplying information about their users to the government, its citizens should be given the right to question the validity of these contracts and their right thereunder. Are citizens of these countries intended to be or legally treated as third-party beneficiaries to these contracts? If so, should individuals have a right to hold the contracting parties accountable for any disproportionate measure undertaken during this time and enforce these breaches as a possible contractual recourse?[155] What other measures can be taken to prevent third-party companies from mining such data for their operational gains?

The choices to be made by governments are those of degree, not of kind. At the very least, the contention of this article is that the government should not put the burden on those under surveillance to actively seek out the data-mining entities and request that their data be deleted. Instead, they should design and monitor a system that justifies the need for data collection and implements the checks and balances required to make it proportional, fair, just and humane. As Glenn Cohen said, “Public health depends a lot on public trust. If the public feels as though they are being misled or misinformed,

their willingness to make sacrifice [is reduced]."[156] Viewed this way, the executive branch of the government must find a delicate balance between the use of technology and data in service of the public good and protecting privacy and avoiding an over-reach on its future uses.

Adam is a senior lawyer with over 12 years of working in the legal and PE industry. Adam specializes in corporate law, M&A and other regulatory and corporate governance matters. Currently, Adam is obtaining an MBA from MIT Sloan focusing on tech entrepreneurship and venture capital.

Footnotes

1. Zeke Emanuel et al., "A National and State Plan To End the Coronavirus Crisis," Center for American Progress, April 3, 2020, https://www.americanprogress.org/issues/healthcare/news/2020/04/03/482613/national-state-plan-end-coronavirus-crisis/. ↩
2. Emanuel et al. ↩
3. Luca Ferretti et al., "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing," *Science* 368, no. 6491 (May 8, 2020), https://doi.org/10.1126/science.abb6936. ↩
4. Emanuel et al., "A National and State Plan To End the Coronavirus Crisis." ↩
5. Umair Irfan, "No Country Has Beaten the Coronavirus Yet," Vox, April 16, 2020, https://www.vox.com/2020/4/16/21215143/coronavirus-covid-19-cases-us-singapore-korea-international-health. ↩
6. Joi Ito, "Supposedly 'Fair' Algorithms can Perpetuate Discrimination" Wired, February 5, 2019 https://www.wired.com/story/ideas-joi-ito-insurance-algorithms/. ↩
7. Korea Centres for Disease Control and Prevention, "Frequently Asked Questions for KCDC on COVID-19 (as of 30 March)," Korea Centres for Disease Control and Prevention, March 30, 2020, https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030. ↩
8. Korea Centres for Disease Control and Prevention. ↩
9. Korea Centres for Disease Control and Prevention. ↩

10. Korea Centres for Disease Control and Prevention. ↩
11. Yonhap News Agency, "S. Korea Set to Launch Quick Tracking System for Virus Cases," Yonhap News Agency, March 25, 2020, https://en.yna.co.kr/view/AEN20200325008300320. ↩
12. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport," Ministry of Land, Infrastructure and Transport, March 26, 2020, http://www.molit.go.kr/english/USR/BORD0201/m_28286/DTL.jsp?id=eng0301&cate=&mode=view&idx=2931&key=&search=&search_regdate_s=&search_regdate_e=&order=&desc=asc&srch_prc_stts=&item_num=0&search_dept_id=&search_dept_nm=&srch_usr_nm=N&srch_usr_titl=N&srch_usr_ctnt=N&srch_mng_nm=N&old_dept_nm=&search_gbn=&search_section=&source=&search1=&lcmspage=1. ↩
13. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport," Ministry of Land, Infrastructure and Transport, March 26, 2002, http://www.molit.go.kr/english/USR/BORD0201/m_28286/DTL.jsp?id=eng0301&cate=&mode=view&idx=2931&key=&search=&search_regdate_s=&search_regdate_e=&order=&desc=asc&srch_prc_stts=&item_num=0&search_dept_id=&search_dept_nm=&srch_usr_nm=N&srch_usr_titl=N&srch_usr_ctnt=N&srch_mng_nm=N&old_dept_nm=&search_gbn=&search_section=&source=&search1=&lcmspage=1. ↩
14. Yonhap News Agency, "S. Korea to Run System to Better Detect Virus Patients' Routes," *Korea Herald*, accessed April 9, 2020, http://www.koreaherald.com/view.php?ud=20200311000132. ↩
15. Sarah Wray, "South Korea to Step-up Online Coronavirus Tracking," Smart Cities World, accessed April 9, 2020, https://www.smartcitiesworld.net/news/news/south-korea-to-step-up-online-coronavirus-tracking-5109. ↩
16. Korea Centres for Disease Control and Prevention. ↩
17. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩
18. Ministry of Land, Infrastructure and Transport. ↩
19. Ministry of Land, Infrastructure and Technology, "MOLIT Ministry of Land, Infrastructure and Transport." ↩

20. Kim, “South Korea Is Watching Quarantined Citizens with a Smartphone App.” ↩
21. Kim. ↩
22. Korea Centres for Disease Control and Prevention, “Enhanced the 2019-NCoV Quarantine Guideline in Republic of Korea,” Korea Centres for Disease Control and Prevention, February 3, 2020, https://www.cdc.go.kr/board/board.es?mid=a30402000000&bid=0030&act=view&list_no=365953&tag=&nPage=15. ↩
23. Kim, “South Korea Is Watching Quarantined Citizens with a Smartphone App.” ↩
24. Max Kim, “South Korea Is Watching Quarantined Citizens with a Smartphone App,” MIT Technology Review, accessed April 9, 2020, https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/. ↩
25. Max Kim, “South Korea Is Watching Quarantined Citizens with a Smartphone App,” MIT Technology Review, accessed April 9, 2020, https://www.technologyreview.com/2020/03/06/905459/coronavirus-south-korea-smartphone-app-quarantine/. ↩
26. Joohee Cho, “Fear Grips Daegu, South Korea, amid Coronavirus,” *ABC News*, accessed April 9, 2020, https://abcnews.go.com/International/fear-grips-daegu-south-korea-amid-coronavirus/story?id=69175021. ↩
27. *COVID-19 Status Map*, accessed April 9, 2020, https://coronamap.site/. ↩
28. “Coronaita,” Coronaita, accessed April 9, 2020, https://coronaita.com. ↩
29. Max S. Kim, “Seoul’s Radical Experiment in Digital Contact Tracing,” The New Yorker, April 17, 2020, https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing. ↩
30. Kim. ↩
31. Mark Zastrow, “South Korea Is Reporting Intimate Details of COVID-19 Cases: Has It Helped?,” *Nature*, March 18, 2020, https://doi.org/10.1038/d41586-020-00740-y. ↩
32. Zastrow. ↩

33. Hyung Eun Kim, "'At a Love Motel': Are S Korea Virus Alerts Too Revealing?," *BBC News*, March 5, 2020, sec. Asia, https://www.bbc.com/news/world-asia-51733145. ↩
34. Min-wook Kim, "□□□□□ □□□□ □□□…□□, '□□□□' □□ □□□ - □□□□ [Self-Isolation Electronic Wristband Controversy over Human Rights Violation]," *JoongAng Daily*, April 7, 2020, https://news.joins.com/article/23749284. ↩
35. Ministry of Government Legislation of South Korea, "□□□□□□□□ | □□□□ > □□ - □□□ □ □□ □ □□□ □□ □□ [Infectious Disease Control and Prevention Act]," Ministry of Government Legislation of South Korea, accessed April 11, 2020, http://www.law.go.kr/LSW/lsInfoP.do?lsiSeq=188080&chrClsCd=010203&urlMode=engLsInfoR&viewCls=engLsInfoR#0000. ↩
36. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩
37. Zastrow, "South Korea Is Reporting Intimate Details of COVID-19 Cases." ↩
38. Zastrow. ↩
39. Hillary Leung, "Hong Kong Sees Record Rise in Coronavirus Cases as New Wave Hits Asia," Time, March 20, 2020, https://time.com/5807097/coronavirus-hong-kong-second-wave/. ↩
40. James Griffiths, "Hong Kong Managed to Contain the Virus, Now It's Worried International Travelers Will Bring It Back," CNN, March 18, 2020, https://www.cnn.com/2020/03/18/asia/hong-kong-coronavirus-second-wave-intl-hnk/index.html. ↩
41. The Hong Kong SAR Government, "COVID-19 Thematic Website, Together, We Fight the Virus, Home Quarantine for Inbound Travellers - Frequently Asked Questions," 2020, https://www.coronavirus.gov.hk/eng/inbound-travel-faq.html. ↩
42. The Hong Kong University of Science and Technology, "HKUST Researchers Develop Smart Geo-Fencing Technology for Home Quarantine amid COVID-19 Pandemic | The Hong Kong University of Science and Technology," The Hong Kong University of Science and Technology, accessed April 9, 2020, https://www.ust.hk/news/research-and-innovation/hkust-researchers-develop-smart-geo-fencing-technology-home-quarantine. ↩

43. The Hong Kong University of Science and Technology. ↩
44. The Hong Kong University of Science and Technology. ↩
45. The Hong Kong University of Science and Technology. ↩
46. The Hong Kong University of Science and Technology. ↩
47. The Hong Kong University of Science and Technology. ↩
48. The Hong Kong University of Science and Technology. ↩
49. The Hong Kong University of Science and Technology. ↩
50. The Government of Hong Kong Special Administrative Region, "OGCIO Sends out SMS Messages for Activating," The Government of Hong Kong Special Administrative Region, accessed April 9, 2020, https://www.info.gov.hk/gia/general/202003/20/P2020032000645.htm. ↩
51. The Government of Hong Kong Special Administrative Region, "OGCIO Sends out SMS Messages for Activating," The Government of Hong Kong Special Administrative Region, accessed April 9, 2020, https://www.info.gov.hk/gia/general/202003/20/P2020032000645.htm. ↩
52. The Hong Kong SAR Government, "CHP Announces No New Local Confirmed Cases of COVID-19 Today," May 5, 2020, https://www.info.gov.hk/gia/general/202005/05/P2020050500506.htm. ↩
53. William Feuer, "Parts of Asia That Relaxed Restrictions without a Resurgence in Coronavirus Cases Did These Three Things," CNBC, May 7, 2020, https://www.cnbc.com/2020/05/07/coronavirus-lessons-learned-in-asia-show-us-is-at-risk-of-a-resurge-in-cases-as-states-reopen-businesses.html. ↩
54. TraceTogether, "TraceTogether," A Singapore Government Agency Website, accessed April 9, 2020, https://www.tracetogether.gov.sg/. ↩
55. TraceTogether, "TraceTogether," A Singapore Government Agency Website, accessed April 9, 2020, https://www.tracetogether.gov.sg/. ↩
56. *Trace Together Application Launched to Support Contact Tracing Process*, accessed April 9, 2020, https://www.facebook.com/watch/?v=869739986772516. ↩

57. The Singapore Government, “Help Speed up Contact Tracing with TraceTogether,” A Singapore Government Agency Website, accessed April 9, 2020, http://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether. ↩
58. The Singapore Government. ↩
59. The Singapore Government. ↩
60. The Singapore Government. ↩
61. The Singapore Government. ↩
62. The Smart Nation and Digital Government Office, “Smart Nation | Press Releases - Launch of New App for Contact Tracing,” The Smart Nation and Digital Government Office, March 20, 2020, https://www.smartnation.gov.sg/whats-new/press-releases/launch-of-new-app-for-contact-tracing. ↩
63. The Government Technology Agency of Singapore, “Responding to COVID-19 with Tech,” March 20, 2020, https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/. ↩
64. Enterprise Singapore, “Frequently Asked Questions on COVID-19,” March 27, 2020. ↩
65. The Parliament of Singapore, “Infectious Diseases Act,” Singapore Statutes Online, accessed April 11, 2020, https://sso.agc.gov.sg/Act/IDA1976. ↩
66.

TraceTogether has several layers of security and privacy safeguards in place. For example, users submit only their mobile numbers after downloading the app.[1] Each phone is assigned a user ID which is used to generate temporary IDs at regular intervals.[2] These temporary IDs are exchanged between the phones of TraceTogether users.[3] This regular generation of temporary IDs protect users from eavesdropping and reduces the ability to conduct tracking by malicious actors.[4] Google Play, “TraceTogether - Apps on Google Play,” Google Play, accessed April 9, 2020, https://play.google.com/store/apps/details?id=sg.gov.tech.bluetrace&hl=en.

---

1. TraceTogether, “TraceTogether.”↩
2. See Kit Tang and Aqil Haziq Mahmud, “Singapore Launches TraceTogether Mobile App to Boost COVID-19 Contact Tracing Efforts,” CNA, March 20, 2020, https://www.channelnewsasia.com/news/singapore/covid19-trace-together-mobile-app-contact-tracing-coronavirus-12560616.↩
3. Tang and Mahmud.↩
4. The Government Technology Agency of Singapore, “9 Geeky Myth-Busting Facts You Need to Know about TraceTogether | Facebook,” March 21, 2020,

↩
67. Apple Store, “TraceTogether,” Apple Store, accessed April 9, 2020, https://apps.apple.com/sg/app/tracetogether/id1498276074. ↩
68. James Vincent, “Spot the Robot Is Reminding Parkgoers in Singapore to Keep Their Distance from One Another,” The Verge, May 8, 2020, https://www.theverge.com/2020/5/8/21251788/spot-boston-dynamics-robot-singapore-park-social-distancing. ↩
69. The Government Technology Agency of Singapore, “NParks and SNDGG Trial SPOT Robot for Safe Distancing Operations at Bishan-Ang Mo Kio Park,” May 8, 2020, https://www.tech.gov.sg/media/media-releases/spot-robot-trial-for-safe-distancing-operations. ↩
70. The Government Technology Agency of Singapore. ↩
71. Office of Guangzhou Municipal People’s Government, “□□□□□□□□□□□□□□□□□□ □□□□□ □□□□377□ [Guangzhou Public Security: Big Data Tracking and Investigation of More than One Million People & Found 377 People with Fever and Other Symptoms],” Office of Guangzhou Municipal People’s Government, accessed April 9, 2020, http://www.gz.gov.cn/xw/jrgz/content/post_5663634.html. ↩
72. Office of Guangzhou Municipal People’s Government. ↩
73. Office of Guangzhou Municipal People’s Government, “□□□□□□□□□□□□□□□□□□ □□□□□ □□□□377□ [Guangzhou Public Security: Big Data Tracking and Investigation of More than One Million People & Found 377 People with Fever and Other Symptoms].” ↩
74. Viola Zhou, “‘Big Data’ segregates millions in China’s coronavirus fight” Inkstone, February 21, 2020, https://www.inkstonenews.com/tech/china-applies-surveillance-technology-big-data-coronavirus-epidemic-control/article/3051754. ↩
75. Zhe Yang, □□, “□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ [How to track confirmed cases? Ouhai District, Wenzhou: Anti-epidemic investigation through big data operators],” *The Paper*, February 3, 2020, https://www.thepaper.cn/newsDetail_forward_5759117. ↩
76. The Ministry of Industry and Information Technology of the People’s Republic of China, “□□□□□□□□□□□□□□□□□□□□‘□□□□’’ [Ministry of Industry and Information Technology Reminder: SMS Can Provide You with “Travel Proof”],’” The Ministry of

Industry and Information Technology, accessed April 9, 2020, http://www.miit.gov.cn/n1146290/n1146402/n1146440/c7681574/content.html. ↩

77. Xuequan Mu, "Over 100 Chinese Cities Adopt QR Codes for Coronavirus Control, Work Resumption," *Xinhuanet*, February 20, 2020, http://www.xinhuanet.com/english/2020-02/20/c_138799637.htm. ↩

78. Mu. ↩

79. The apps rely heavily on self-reporting, including a person's medical records, travel history and whether he/she has been in contact with someone diagnosed with the virus. ↩

80. QiaoSu Zhang, □□□, "□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□ [Realize the Mutual Communication and Recognition of Epidemic Prevention Health Codes in Multiple Chinese Cities]," *Xinhuanet*, March 18, 2020, http://www.xinhuanet.com/legal/2020-03/18/c_1125727318.htm. ↩

81. Sophia Ankel, "As China Lifts Its Coronavirus Lockdowns, Authorities Are Using a Color-Coded Health System to Dictate Where Citizens Can Go. Here's How It Works," Business Insider, accessed April 9, 2020, https://www.businessinsider.com/coronavirus-china-health-software-color-coded-how-it-works-2020-4. ↩

82. QiaoSu Zhang, □□□, "□□□□□□□□□□□□□□ □□□□□□□□□□□□□□□□□□□□ [Realize the Mutual Communication and Recognition of Epidemic Prevention Health Codes in Multiple Chinese Cities]," *Xinhuanet*, March 18, 2020, http://www.xinhuanet.com/legal/2020-03/18/c_1125727318.htm. ↩

83. Paul Mozur, Raymond Zhong, and Aaron Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags," *The New York Times*, March 1, 2020, sec. Business, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. ↩

84. Helen Davidson, "China's Coronavirus Health Code Apps Raise Concerns over Privacy," *The Guardian*, April 1, 2020, sec. World news, https://www.theguardian.com/world/2020/apr/01/chinas-coronavirus-health-code-apps-raise-concerns-over-privacy. ↩

85. Helen Davidson, "China's Coronavirus Health Code Apps Raise Concerns over Privacy," *The Guardian*, April 1, 2020, sec. World news ↩

86. QingZhao Li, □□□, "□□□□□□□□□□□ [Tencent Health Code Uses Technology to Prevent Pandemic]," *Xinhuanet*, February 19, 2020, http://www.gd.xinhuanet.com/newscenter/2020-02/19/c_1125595800.htm. ↩
87. QingZhao Li, □□□, "□□□□□□□□□□□ [Tencent Health Code Uses Technology to Prevent Pandemic]," *Xinhuanet*, February 19, 2020 ↩
88. QingZhao Li, □□□. ↩
89. Kari Soo Lindberg and Jinshan Hong, "People in China Need a Green Light From Alipay App to Move Around Country," *Bloomberg.Com*, March 23, 2020, https://www.bloomberg.com/news/articles/2020-03-23/to-pass-go-in-china-you-need-a-green-light-from-alipay-app. ↩
90. Mozur, Zhong, and Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." ↩
91. Mozur, Zhong, and Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags." ↩
92. Di Wang, □□, "□□□□□□□□□□□□□□□'□□'——'□□□'□□□□□□ [I Have Seen Hangzhou at Four in the Morning, Just for an Early 'No Code'-the Recovery Record behind the 'Health Code']," *Xinhuanet*, February 21, 2020, http://www.xinhuanet.com/2020-02/21/c_1125607497.htm. ↩
93. Hangzhou Public Security Bureau, "□□'□'□□□□□□□□□□'□□□'□'□□'□□□□□□[Fighting against the Pandemic, [Communist] Party Members Are in Action □The Public Security Have a 'Tough' Role (1)]," WeChat Official Accounts Platform, accessed April 9, 2020, http://mp.weixin.qq.com/s?__biz=MzA4MjM2MDgxMA==&mid=2815608170&idx=1&sn=665c2ec6b676030d263007aae2127c0f&chksm=bda085ef8ad70cf9e84bdb3b59f4d1cdcd2a3e467d25dffe9219f54f4db160281881e5d57817#rd. ↩
94. World Health Organization, "COVID-19 Situation Reports," May 9, 2020, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports. ↩
95. The United States Department of Health and Human Services, "Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA)

Privacy Rule," Text, HHS.gov, September 7, 2012, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html. ↩
96. The Centers for Disease Control and Prevention, "HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services*," The Centers for Disease Control and Prevention, accessed April 12, 2020, https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm. ↩
97. The New York Times, "Coronavirus in the U.S.: Latest Map and Case Count," *The New York Times*, April 9, 2020, sec. U.S., https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html. ↩
98. Thomas Fuller, "How Much Should the Public Know About Who Has the Coronavirus?," *The New York Times*, March 28, 2020, sec. U.S., https://www.nytimes.com/2020/03/28/us/coronavirus-data-privacy.html. ↩
99. Thomas Fuller, "How Much Should the Public Know About Who Has the Coronavirus?," *The New York Times*, March 28, 2020, sec. U.S. ↩
100. Ministry of Health, Singapore, "MOH | Updates on COVID-19 (Coronavirus Disease 2019) Local Situation," May 9, 2020, https://www.moh.gov.sg/covid-19. ↩
101. Fuller. ↩
102. Moritz Kraemer, "I'm a Researcher Who's Helped Change How We Tackle Pandemics like Coronavirus – This Is What We've Learned," The Independent, March 17, 2020, https://www.independent.co.uk/voices/coronavirus-covid-19-pandemic-outbreak-data-research-cdc-who-a9406281.html. ↩
103. Kraemer. ↩
104. Samantha Fry et al., "Quarantine and Isolation Authorities in States Affected by COVID-19," Lawfare, March 6, 2020, https://www.lawfareblog.com/quarantine-and-isolation-authorities-states-affected-covid-19. ↩
105. Connecticut Department of Public Health, "Laboratory-Confirmed Cases by Town" accessed May 17, 2020. https://portal.ct.gov/Coronavirus. ↩
106. Florida Department of Health, Division of Disease Control and Health Protection, "Florida's COVID-19 Data and Map Dashboard," Florida's COVID-19 Data

and Surveillance Dashboard, accessed April 10, 2020, https://experience.arcgis.com/experience/96dd742462124fa0b38ddedb9b25e429. ↩
107. Florida Department of Health, Division of Disease Control and Health Protection, "2019 Novel Coronavirus Response (COVID-19)," Florida Department of Health COVID-19 Outbreak, accessed April 10, 2020, https://floridahealthcovid19.gov/. ↩
108. Fuller, "How Much Should the Public Know About Who Has the Coronavirus?" ↩
109. John Hopkins University & Medicine Coronavirus Resource Center, "COVID-19 Cases by US-County" accessed May 17, 2020 https://coronavirus.jhu.edu/us-map. ↩
110. The European Commission, "EC Recommendation on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis," The European Commission, April 8, 2020. ↩
111. "European Commission on a Common Union Toolbox for the Use of Technology and Data to Combat and Exit from the COVID-19 Crisis, in Particular Concerning Mobile Applications and the Use of Anonymised Mobility Data," accessed April 9, 2020, https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf. ↩
112. Natasha Lomas, "Telco Metadata Grab Is for Modelling COVID-19 Spread, Not Tracking Citizens, Says EC," *TechCrunch* (blog), accessed April 9, 2020, https://social.techcrunch.com/2020/03/27/telco-metadata-grab-is-for-modelling-covid-19-spread-not-tracking-citizens-says-ec/. ↩
113. Oleg Magni, "Deploying Cellphone Data to Fight COVID-19," Inserm Research Institute, March 27, 2020, https://presse.inserm.fr/en/deploying-cellphone-data-to-fight-covid-19/38831/. ↩
114. Manuel Rosa-Calatrava, "Inserm's Commitment to the Fight against the Covid-19 Pandemic," Newsroom | Inserm, April 22, 2020, https://presse.inserm.fr/en/inserm-fully-committed-to-the-fight-against-the-covid-19-pandemic/39221/. ↩
115. The European Data Protection Board, "Statement of the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak," Press Release, The European Data Protection Board, March 16, 2020, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid-19_20200316_press_statement_en.pdf. ↩

116. The European Data Protection Board, "Statement of the EDPB Chair on the Processing of Personal Data in the Context of the COVID-19 Outbreak," Press Release, The European Data Protection Board, March 16, 2020, https://edpb.europa.eu/sites/edpb/files/files/news/edpb_covid-19_20200316_press_statement_en.pdf. ↩
117. The European Data Protection Board. ↩
118. Lomas, "Telco Metadata Grab Is for Modelling COVID-19 Spread, Not Tracking Citizens, Says EC." ↩
119.
In Germany, which has some of Europe's strictest data privacy protections due to its unique political regime, the government can compel a technology company to share location data on an individual in the interest of national security.[1] However, indiscriminate mass tracking of individuals generally lacks a legal basis. To track people who have or might have coronavirus, Germany and other European countries would need to pass laws specifying how data collection would be restricted to a certain population, for a certain time, and for a certain purpose.[2] [3] Christian Geinitz, "Gefahrenabwehr: Bund Will Länder in Der Corona-Bekämpfung Entmachten [Federal Government Wants to Disempower States in the Fight against Coronavirus]," *Frankfurter Allgemeine Zeitung*, March 21, 2020, https://www.faz.net/1.6689784.

---

1. Dotmagazine, "Germany: Land of Data Protection and Security – But Why?," Dotmagazine, accessed April 9, 2020, https://www.dotmagazine.online/issues/security/germany-land-of-data-protection-and-security-but-why.↩
2. Dotmagazine.↩
3. Kelly Servick, "Cellphone Tracking Could Help Stem the Spread of Coronavirus. Is Privacy the Price?," American Association for the Advancement of Science, March 22, 2020, https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price.↩

↩
120. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩

121. Brian Kim, “Lessons for America: How South Korean Authorities Used Law to Fight the Coronavirus,” Lawfare, March 16, 2020, https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus. ↩
122. Korea Centres for Disease Control and Prevention, “Frequently Asked Questions for KCDC on COVID-19 (as of 30 March).” ↩
123. Kim, “Lessons for America.” ↩
124. Personal Data Protection Commission of Singapore, “PDPC | Advisory on Collection of Personal Data for COVID-19 Contact Tracing,” Personal Data Protection Commission of Singapore, accessed April 11, 2020, https://www.pdpc.gov.sg/Help-and-Resources/2020/03/Advisory-on-Collection-of-Personal-Data-for-COVID-19-Contact-Tracing. ↩
125. The Parliament of Singapore, “Personal Data Protection Act 2012,” Singapore Statutes Online, accessed April 11, 2020, https://sso.agc.gov.sg/Act/PDPA2012. ↩
126.
Like Singapore, the Personal Data (Privacy) Ordinance (PDPO) in Hong Kong stipulates exceptions in emergency health situations to the general rule that personal data cannot be used or disclosed for a purpose other than the original purpose of its collection. These exceptions can be considered to have taken effect as COVID-19 has been added as one of the notifiable infectious diseases under the Prevention and Control of Disease Ordinance.[1] Section 59 of the PDPO provides for the situations where the use of personal data may be exempted from the relevant data protection principles if it relates to safeguarding the physical or mental health concerns of the data subject or overall public interests. The Office of the Privacy Commissioner for Personal Data, “The Use of Information on Social Media for Tracking Potential Carriers of COVID-19.”

---

1. The Office of the Privacy Commissioner for Personal Data, “The Use of Information on Social Media for Tracking Potential Carriers of COVID-19,” The Office of the Privacy Commissioner for Personal Data, February 26, 2020, https://www.pcpd.org.hk/english/news_events/media_statements/press_20200226.html.↩

↩

127.
Due to the time pressure to carry out these measures, the use of legislative apparatus is by no means a legally hermetical avenue to action. For example, in the EU, the ePrivacy Directive was promulgated in 2002 and amended in 2009. The EU had intended to replace it alongside an update to the broader personal data protection framework under the ePrivacy Regulation. Other general aims for ePrivacy Regulation include strengthening the rules around the privacy of electronic communications and the tracking of Internet users more broadly, as well as combatting problems such as spam, profiling and behavioral advertising by requiring transparency and affirmative consent.[1] However, the precise scope of the proposed regulations remains a hotly-debated area among EU member states, with critics arguing that the regulation could have a disproportionate impact if every app with a communication functionality (i.e. a chat function) falls under the new regime. Chief among them is the presumed exploitation of consumers' online activities, which ePrivacy seeks to regulate and which is already deeply ingrained in the dominant digital business modus operandi. Any legislative attempt to impose overarching regulations over the business model of digital giants such as Facebook will likely invite coordinated industry complaints.[2] Lomas, "Telco Metadata Grab Is for Modelling COVID-19 Spread, Not Tracking Citizens, Says EC."

---

1. The European Commission, "Proposal for a Regulation on Privacy and Electronic Communications," Text, The European Commission, January 10, 2017, https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.↩
2. Natasha Lomas, "EPrivacy: An Overview of Europe's Other Big Privacy Rule Change," Techcrunch, October 7, 2018, https://techcrunch.com/2018/10/07/eprivacy-an-overview-of-europes-other-big-privacy-rule-change/.↩

↩

128. Fuller, "How Much Should the Public Know About Who Has the Coronavirus?" ↩

129. Lydia F. de la Torre, "What Does 'Data Protection by Design and by Default' Mean under EU Data Protection Law?," Medium, December 8, 2019, https://medium.com/golden-data/what-does-data-protection-by-design-and-by-default-mean-under-eu-data-protection-law-fc40f585c0c5. ↩

130. Nicholas Vollmer, "Article 35 EU General Data Protection Regulation (EU-GDPR)," text (SecureDataService, September 5, 2018), 35, https://www.privacy-regulation.eu/en/article-35-data-protection-impact-assessment-GDPR.htm. ↩
131. Mireille Hildebrandt, "10. 'Legal by Design' or 'Legal Protection by Design'?," in *Law for Computer Scientists* (PubPub, 2019), https://lawforcomputerscientists.pubpub.org/pub/gfzd6k0g/release/12. ↩
132. Nicholas Vollmer, "Article 25 EU General Data Protection Regulation (EU-GDPR)," text (SecureDataService, September 5, 2018), 2, https://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm. ↩
133. Ramesh Raskar, "Private Kit: Safe Paths; Privacy-by-Design Contact Tracing Using GPS+Bluetooth | Safepaths," MIT Safepaths, accessed April 9, 2020, http://safepaths.mit.edu/. ↩
134. Ramesh Raskar, "Private Kit: Safe Paths; Privacy-by-Design Contact Tracing Using GPS+Bluetooth | Safepaths," MIT Safepaths ↩
135. Ramesh Raskar, "Private Kit: Safe Paths; Privacy-by-Design Contact Tracing Using GPS+Bluetooth | Safepaths," MIT Safepaths ↩
136. Ramesh Raskar, "Private Kit: Safe Paths; Privacy-by-Design Contact Tracing Using GPS+Bluetooth | Safepaths," MIT Safepaths ↩
137. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩
138. Fraunhofer Heinrich Hertz Institute, HH, "Privacy Protecting Proximity Tracing to Fight Corona – Fraunhofer Heinrich Hertz Institute," Fraunhofer Heinrich Hertz Institute, HHI, accessed April 10, 2020, https://www.hhi.fraunhofer.de/en/press-media/news/2020/privacy-protecting-proximity-tracing-to-fight-corona.html. ↩
139. Douglas Busvine, "Germany Aims to Launch Singapore-Style Coronavirus App in Weeks," *Reuters*, March 30, 2020, https://www.reuters.com/article/us-health-coronavirus-germany-tech-idUSKBN21H26Z. ↩
140. Sophie in 't Veld, "Tweeter Post," Twitter, March 25, 2020, https://twitter.com/sophieintveld/status/1242763831572480006?ref_url=https%3a%2f%2ftechcrunch.com%2f2020%2f03%2f27%2ftelco-metadata-grab-is-for-modelling-covid-19-spread-not-tracking-citizens-says-ec%2f. ↩

141. Jenny Colgate, "Can You Find Me Now? Location Privacy and the Coronavirus Pandemic," *Lexology*, accessed April 9, 2020, Retrieved from https://www.lexology.com. ↩
142. Wojciech Wiewiórowski, "Letter from EDPS to EC: Monitoring Spread of COVID-19," March 25, 2020. ↩
143. Natasha Lomas, "Researchers Spotlight the Lie of 'Anonymous' Data," Techcrunch, accessed April 10, 2020, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/. ↩
144. Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models," *Nature Communications* 10, no. 1 (July 23, 2019): 1–9, https://doi.org/10.1038/s41467-019-10933-3. ↩
145. Rocher, Hendrickx, and de Montjoye. ↩
146. Lomas, "Telco Metadata Grab Is for Modelling COVID-19 Spread, Not Tracking Citizens, Says EC." ↩
147. Wiewiórowski, "Letter from EDPS to EC: Monitoring Spread of COVID-19," March 25, 2020. ↩
148. Gauthier Chassang, "The Impact of the EU General Data Protection Regulation on Scientific Research," *Ecancermedicalscience* 11 (January 3, 2017), https://doi.org/10.3332/ecancer.2017.709. ↩
149. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩
150. Ministry of Land, Infrastructure and Transport, "MOLIT Ministry of Land, Infrastructure and Transport." ↩
151. Yuval Noah Harari, "Yuval Noah Harari: The World after Coronavirus," Financial Times, March 20, 2020, https://amp.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75. ↩
152. Yuval Noah Harari, "Yuval Noah Harari: The World after Coronavirus," Financial Times, March 20, 2020. ↩

153. United Nations Human Rights Office of the High Commissioner, "COVID-19: Governments Must Promote and Protect Access to and Free Flow of Information during Pandemic – International Experts," Office of the United Nations High Commissioner for Human Rights, March 19, 2020, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25729&LangID=E. ↩

154. Thomas Fuller, "How Much Should the Public Know About Who Has the Coronavirus?," *The New York Times*, March 28, 2020, sec. U.S., https://www.nytimes.com/2020/03/28/us/coronavirus-data-privacy.html. ↩

155. Colgate, "Can You Find Me Now?" ↩

156. Fuller, "How Much Should the Public Know About Who Has the Coronavirus?" ↩