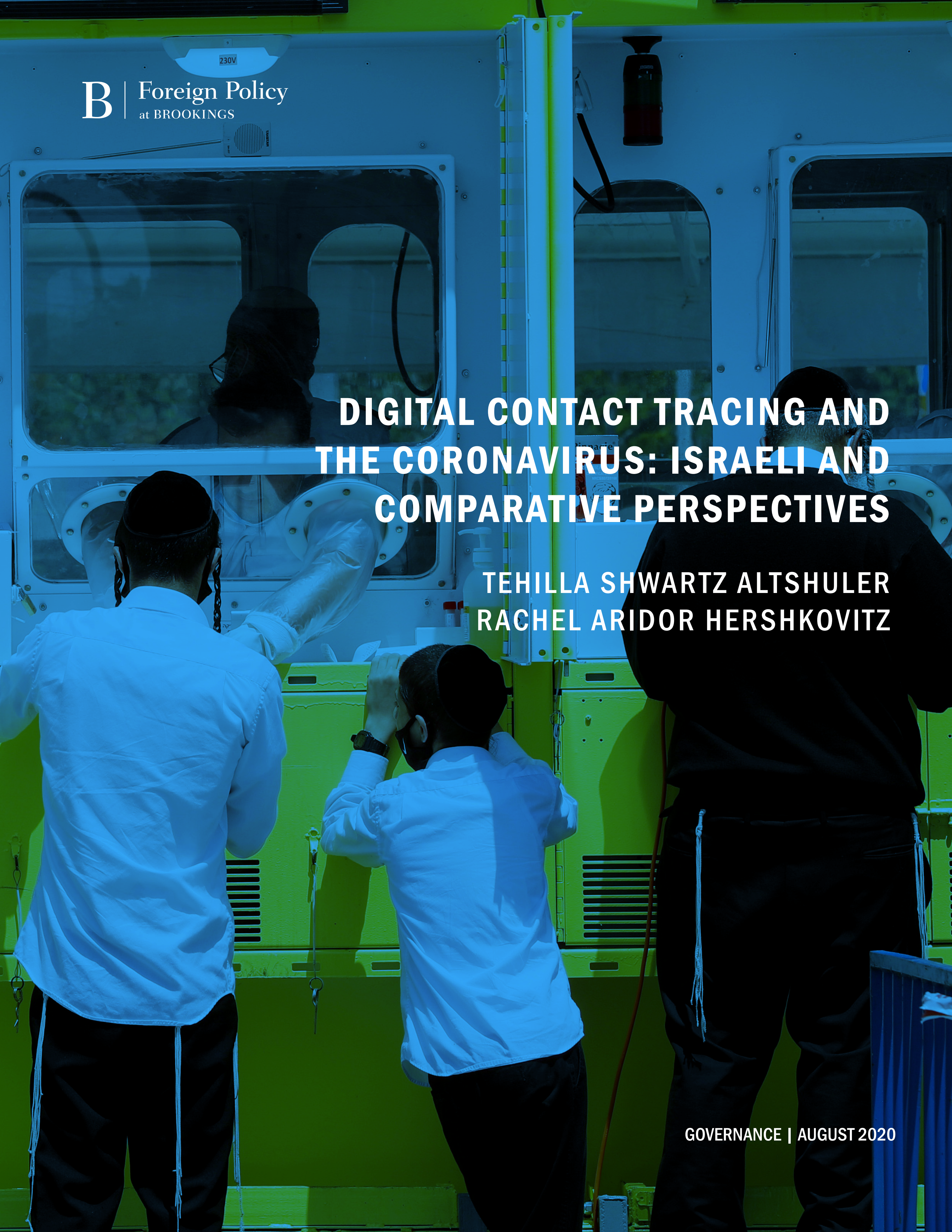
Foreign Policy
at BROOKINGS



DIGITAL CONTACT TRACING AND THE CORONAVIRUS: ISRAELI AND COMPARATIVE PERSPECTIVES

TEHILLA SHWARTZ ALTSHULER
RACHEL ARIDOR HERSHKOVITZ

GOVERNANCE | AUGUST 2020

DIGITAL CONTACT TRACING AND THE CORONAVIRUS: ISRAELI AND COMPARATIVE PERSPECTIVES

TEHILLA SHWARTZ ALTSHULER
RACHEL ARIDOR HERSHKOVITZ

EXECUTIVE SUMMARY

Digital contact tracing is the main technological issue currently facing countries that are dealing with the COVID-19 pandemic. This paper explains the concept of digital contact tracing and highlights its importance as a helpful tool for human epidemiological investigations and for minimizing the spread of the novel coronavirus. It goes on to survey the international scale of policy tools that have been selected for the purpose of digital contact tracing — ranging from China, which imposed mandatory means on all citizens that incorporate artificial intelligence and generate a "health code"; to Asian democracies such as South Korea and Taiwan, which have implemented intrusive digital tracking tools that are run by civil agencies, with no involvement of the secret services; to the democratic countries of Europe as well as Australia, New Zealand, and the United States, which employ digital contact tracing only with citizens' consent. Israel, it was found, has positioned itself between the Asian democracies and China.

We believe that a new outbreak of the pandemic in the winter of 2020-2021 is liable to prompt countries to choose one of two options. The first is to refrain from using digital contact-tracing technology because of its infringement on privacy. We believe this would be the wrong choice, because it means losing a major technological advantage for coping with the virus and would merely reinforce the mistaken argument that privacy and innovation are incompatible. The second option, which we suspect would be adopted by "weak democracies," is comprehensive involuntary digital contract tracing, in which the data is collected from cellular providers for centralized processing, relying in part on security agencies and secret services.

To avoid falling into the second scenario, which would deal a serious blow to the right to privacy and to human rights in general, we propose an intermediate model that can provide solutions to the problems that arise in the use of cellphone apps for contact tracing. Our proposal is that countries adopt apps specifically designed for digital contact tracing and that derive their data from users' personal devices, with their

consent, and then make use of the information solely for contact tracing if a user tests positive for the coronavirus. The information extracted from the app would be limited not only with regard to the purpose for which it is used, but also with regard to who is permitted to access it — that is, only civilian government agencies with no investigative and enforcement powers. Governments must make special efforts to encourage the public to install the app, with full transparency. In addition, steps must be taken to devise solutions for population groups that do not use smartphones, such as by means of smartcards designed for this purpose or of wearable technology that can receive and transmit Bluetooth signals.

INTRODUCTION

The coronavirus pandemic generated an unprecedented global crisis that illustrates Thomas Hobbes' statement that *fear* of death is a very strong political motive.[1] This fear prompted citizens of all democratic countries to obey orders and voluntarily surrender some of their basic freedoms, in exchange for maintaining their health. In parallel, the very same fear has led democratic governments to place restrictions on freedom, demonstrating their immense power and control, in ways which would have been deemed quite inconceivable before the pandemic.

Note, however, that not all countries have wielded this power to the same degree. To a great extent, the coronavirus crisis has revealed the strengths and weaknesses of democratic regimes in various countries — as illustrated by the technological solutions that various countries have proposed, discussed, and selected, as tools for dealing with the pandemic. The overlap between the pandemic and these technologies has demonstrated once again that technology is by no means neutral, and is in fact a political, social, and cultural issue. Although we are still only midway through the outbreak, and the world is still finding its way into a coronavirus routine, now is the time to investigate the variations from country to country and draw some initial conclusions, using Israel as our case study.

The present paper focuses on the use of digital contact tracing to track the coronavirus chain of infection, identify those who have come into contact with a confirmed COVID-19 patient, and send him or her into quarantine. This is the main technological issue countries face today as they deal with the pandemic. We will explain what digital contact tracing is, why it is necessary, and how it is carried out in Israel as compared to other countries.

CONTACT-TRACING TECHNOLOGIES AND WAYS TO IMPLEMENT THEM

Contact tracing is geared to identifying individuals who have been in physical proximity to a confirmed COVID-19 patient, in order to facilitate their rapid isolation, on the assumption that there is a strong likelihood that they have been infected. Proximity to a confirmed patient is determined on the basis of epidemiological indicators — the duration of the exposure and the distance from the source of infection. Scientific papers and field reports suggest that digital contact tracing can make a major contribution to the war against the coronavirus pandemic and can serve as a vital supplement to traditional human epidemiological studies. It is particularly effective for identifying persons who were near “super-spreaders” — that is, confirmed patients who spent a long time near many people, in high-risk venues such as public transportation, supermarkets, houses of worship, and places of entertainment. The authorities’ ability to identify those who were in the vicinity of a super-spreader and order them to go into quarantine is one of the most effective methods for limiting transmission of the virus.[2]

Digital contact tracing is put in place when physical proximity is inferred through collecting and analyzing data from citizens’ mobile devices, including cellphone location data, close contact between users as determined by means of Bluetooth Low Energy (BLE) signals, and other technologies (such as acoustic communication).[3]

Cellphone location data can be collected in bulk from the cellular network, since it is stored on the cellular devices of those users who permit this, but also from the cellular providers, even without users’ permission. As a result, intelligence and security agencies can make use of cellphone location data without users’ knowledge.

BLE signals do not provide any information about a user’s location or movements and are stored only on the user’s own device. With regard to protecting users’ privacy, this method thus has an inherent advantage over cellular location data. On the other hand, because it is difficult to collect in bulk, its use for digital contact tracing is more limited, preventing public health authorities from acquiring a precise and up-to-date snapshot of the extent of exposure to confirmed COVID-19 patients and determining who must enter quarantine.

Another consideration is that cellphone localization is less precise than BLE, because of the size of the mobile communication cells and the fact that Global Positioning System-based location data may be affected by weather conditions or physical perturbations. Cellphone localization also does a poor job at identifying vertical proximity, and consequently is not precise in skyscrapers and closed shopping malls — the architecture typical of cities and dense urban environments where COVID-19 is most likely to spread. This is why effective digital contact tracing based on cellphone location data must also make use of supplementary information (such as users’ call, message, and browsing histories) and human epidemiological studies.[4]

In addition, achieving the goal of contact tracing does not require tracking the spatial movements of COVID-19 patients, but rather just knowing who was physically close to them, on the basis of epidemiological indicators.[5] So it is not necessary to know precisely when (day and time) a person arrived in a particular geographical location. It is sufficient to know the date and how long the person remained close to nearby cellular devices. For this reason, from the perspective of data minimization — collecting as little personal data as possible, as stipulated, for example, by the European General Data Privacy Regulations (GDPR) — reliance on BLE signals is preferable.[6]

There are two main forms of digital contact tracing. The first relies on centralized acquisition of cellphone location data from cellular providers in a particular country. The information is fed into a data pool and is then processed. The processing can be performed by a civilian government agency — such as the healthcare authorities — or by security agencies that enjoy direct access to the cellular infrastructure in order to protect national security and prevent terrorism and crime — such as the Israeli General Security Service (GSS). The processing can be carried out by creating in-house expertise within these agencies, or by private firms on secured government servers.

For example, the Israeli firm NSO Group Technologies offers Fleming, an analytics system developed in cooperation with the Israeli defense establishment. Fleming offers diverse services, including contact tracing, hot-spot mapping, and forecasting of outbreaks. It can also identify and localize chains of infections by super-spreaders and generate an individual score for a person's potential for infection if exposed to a confirmed patient. This system does not collect the information, but rather is applied to information stored on the healthcare agencies' servers, integrated with cellphone location data from the cellular providers. The product has been offered to the Ministry of Defense in Israel and to European countries.[7]

The technology company Palantir is cooperating with the British Startup Faculty to provide analytical, processing, and data-display services to the National Health Service (NHS) in the United Kingdom. The information is not collected by the companies, but rather-by the medical services themselves and by other organizations, and is stored on NHS data servers. The agreement between the NHS and Palantir has been published, as well as the NHS's commitment to delete the information from its servers when the crisis is over.[8]

The advantage of this method is that a government is able to conduct centralized monitoring of the entire population and generate lists of those who must be quarantined. Its clear disadvantage is the broad, involuntary infringement of citizens' privacy when the authorities collect extensive information about the whereabouts and the call and text-message histories of the entire population.[9]

Of course, analysis of the data by the healthcare authorities or by private companies on behalf of the healthcare authorities, in accordance with their demands and under their supervision, is preferable to having the data processed by intelligence organizations. This for several reasons. One is the importance of transparency — as well as public and judicial oversight — of the scope of the technological capacity, data collection, and the use made of it. Another is the fact that the healthcare authorities are not an investigative and enforcement body, meaning that there is no fear that information they acquire will be used for law enforcement. On the other hand, the intelligence agencies, at least in some countries, already possess the technological skills for carrying out this task immediately, and at a much higher level of data security than civilian agencies can guarantee.

The second main form of digital contact tracing is based on made-to-order apps. The installation of such contact-tracing apps on individuals' devices may be voluntary or mandatory, and their architecture may be centralized or decentralized.[10]

The main debate over the use of such apps has to do with the degree of centralization. A centralized approach means that if a user tests positive for the coronavirus and voluntarily informs the app, the contact data that the app has stored on the user's phone is transmitted to the national healthcare agency, where it is decoded and processed. A decentralized approach involves sending the information directly to the other users of the app, in which case the data is decoded and processed on each user's cellular device.

Most democracies that have chosen to use digital contact tracing executed it via a voluntarily installed contact-tracing app. Most of them opted for a decentralized architecture app due to a rare instance of cooperation between Google and Apple which demanded it as a precondition.[11] The two tech giants released in mid-May an application programming interface (API) that makes it possible to develop and install apps that rely on the operating system's background Bluetooth signals. The companies stated that the new API would be available only to contact-tracing apps operated by or for governments or healthcare services, as part of the battle against the spread of the novel coronavirus, and would support only the decentralized approach.[12] The positive side of the decentralized architecture — namely, allowing users to choose whether to forward the data to the authorities — has already influenced several countries, including Italy, Germany, Switzerland, and several states in the United States.[13]

Nevertheless, the ramifications of this rare cooperation should also be noted. In fact, it expropriates the decision-making power regarding digital contact tracing away from the hands of governments, since not complying with Apple and Google requirements may impede the efficiency and effectiveness of the apps. Especially in Apple's smartphones, these apps drain the devices' battery and stop working whenever the device is locked or in sleep mode. France, Australia, and Singapore insisted on centralized digital contact tracing apps, emphasizing the need for app's sovereignty and the importance of public health authority's ability to know who was in physical proximity to a person with COVID-19 and therefore may be exposed to the virus.[14] However, the apps they developed did not comply with Google and Apple requirements and therefore could not run in the background of the iOS operating system.[15] In Singapore, it caused people to uninstall the app, leading the country to seek other solutions, such as providing people a smart token if needed.[16] Australia and France face claims regarding the inefficiency of their apps in providing accurate contact tracing. France's app, for example, managed to identify and warn only 14 people in its first three weeks, despite being downloaded by 2 million people in a short time.[17] It seems, therefore, that governments must either find a way to evade Google and Apple requirements or to avoid using BLE for their contact tracing technology. New Zealand, for example, released a Bluetooth-free contact tracing app that generates a digital record of public places a citizen visited by using QR codes.[18]

Digital contact-tracing apps offer a number of advantages, including protecting users' privacy at various levels; avoiding mass involuntary tracking; making users aware of the infringement of their privacy; and giving users control of the app's various functions.

However, the app method has two major downsides. The first is that if the app does not upload data to a central server, a country lacks any tools to determine who must be sent into quarantine and to monitor their compliance.[19] The second disadvantage is that the app makes it possible to trace contacts and notify only those who have installed it, and not the population as a whole. For this reason, major efforts must be invested in broad advertising campaigns to encourage the public to install the app.[20]

It is estimated that if 56% of the population in a country were to install the app, it may be sufficient for controlling the pandemic on its own, without any other form of intervention. However, much lower levels of app adoption could still be vitally important for tackling COVID-19.[21] Another factor is the penetration of smartphones. In Israel, for example, where the ultra-Orthodox have religious scruples against the use of smartphones, approximately 600,000 of the six million cellphone owners in the country have only "dumb phones."[22]

The government of India has required certain sectors of the population — such as essential workers, civil servants, and residents of regions defined as at high-risk for outbreaks — to install contact-tracing apps. Employers and residential compound managers in areas at risk are responsible for verifying that the app has been installed.[23] In New Zealand, it has been proposed to distribute special smartcards to the entire population in order to enable contact tracing, as a way to get around the need to install an app.[24]

As time passes, there has been growing criticism of the use of technology-based contact-tracing methods. First of all, the weaknesses noted here mean that they cannot be relied on as a tool, and certainly not as the only tool, for deciding whether to stay home or go out and risk exposure to the virus. Some critics go further and assert that the technology provides a false sense of security that exceeds its capabilities.[25] Second, epidemiologists maintain that despite the temptation to make contact tracing automatic and technology-based, there is no substitute for human epidemiological studies, which are the only way to provide a full answer to the need to close the chain of infection and identify candidates for testing and quarantine.[26] It is clear, then, that the main criticism of the method is the fear of misuse of the data, infringements of privacy, and heightened government surveillance of citizens.[27]

Indeed, from a normative perspective, any digital contact-tracing technology provides a government with the ability to track various aspects of its citizens' lives and habits is problematic, because it has the potential to be used for mass surveillance.[28] This is especially troubling when the digital contact-tracing technology is based on location data, which can provide its collector — the government — with extremely sensitive personal information about its citizens.[29]

> **“The right to privacy is not absolute. It must be balanced against other interests, rights, and values.**

However, as any basic human right, the right to privacy is not absolute. It must be balanced against other interests, rights, and values. With respect to digital contact-tracing technologies, the main question is, therefore: What is the correct balance between the right to privacy and the right to health?[30] The correct balance should be implemented via the principle of "privacy by design" — that is, examining the ramifications of digital contact-tracing technology for the appropriate balance at each stage of that information's life, from collection to processing to transfer to the authorities, for use in the fight against the spread of COVID-19.

THE DIGITAL CONTACT-TRACING SCALE

In a review we conducted to compare Israel to other countries, we looked at the policy instruments they have selected to permit digital contact tracing. We studied several European Union (EU) countries, the United Kingdom, several Asian countries (both democracies, South Korea and Taiwan, and those that are not democratic, Singapore and China), Australia, New Zealand, and the United States.

We compared the policy instruments each country implemented for the purpose of contact tracing and its rank on Freedom House's "Global Freedom Scores" index, so as to investigate whether stronger democracies choose less invasive methods; the existence of explicit and up-to-date legislation for dealing with pandemics, which could reflect an organized structure of monitoring methods to deal with pandemics; the existence of up-to-date privacy protection legislation that incorporates standards and directives for tracking citizens during states of emergency; other restrictive means, in addition to contact-tracing, that have been imposed, such as quarantines and lockdowns; and the morbidity and mortality rates in each country.[31]

A survey of countries that have been employing contact-tracing technologies allows us to construct a scale. At one extreme is China. In China, the tracking of coronavirus patients was based on the means used to monitor all citizens in routine times. Cellular providers already forwarded their customers' location data to the authorities, and surveillance cameras in public areas (supported by facial recognition based on artificial intelligence) make it possible to identify pedestrians, even if they are wearing a mask, and to estimate their body temperature. The close ties between the e-commerce giant Alibaba and the central government soon produced an application that all Chinese citizens have been required to install on their phones. The application can compute a health code for every citizen, based on an algorithm that weights the identities of all persons with whom they have come into contact, the places they have visited, and their symptoms. The health code, in turn, determines who is allowed to circulate in the public space and who is required to stay at home.[32]

At the other end of the scale are the European Union and countries that are bound by the GDPR and the EU's electronic privacy directives. These provide that cellphone location data may be collected only with the consent of those tracked or in anonymized fashion — that is, in a way that makes it impossible for the authorities to associate a particular person with his or her location data. Deviations from this rule are permitted in an emergency, but only in a proportionate and democratic fashion.[33]

Because of these EU regulations, Italy[34] initially enforced lockdown and quarantine orders only on the basis of reports by concerned neighbors and police patrols. The Italian cellphone providers (Telecom Italia, Vodafone, and WindTre) passed on only anonymous and statistical cellphone location data to the authorities, which made it possible to map large assemblies of people but not to locate individuals.[35] However, with the end of the lockdown and gradual renewal of normal activity in the country, the Italian government released an app named Immuni to permit voluntary contact tracing based on BLE signals, with a decentralized architecture.[36]

In Germany, too,[37] the legislation on pandemics subjects the collection and processing of individual data to the stipulations of the GDPR.[38] The German Data Protection Commission emphasized that government access to the cellphone location data of confirmed patients or those in quarantine is problematic.[39] At first, Germany did not go further than having Deutsche Telekom transmit anonymous and aggregate location data to the authorities. Now that the lockdown is ending, however, the German government also released a voluntary contact-tracing app based on BLE signals and a decentralized architecture.[40]

Switzerland,[41] the United Kingdom,[42] and Austria[43] released a voluntary contact-tracing app based on BLE signals and employing the decentralized approach.[44] France[45] worked in the same direction and developed a technological tool that is intended to ease the lockdown and return to normal economic activity. France's app employs BLE signals, but has a centralized architecture.[46]

New Zealand[47] closed its borders and imposed mandatory and strictly enforced quarantines for all visitors, with widespread lockdowns and social distancing measures. It began using digital contact-tracing technologies only when it reopened the economy, by means of NZ COVID Tracer, a voluntary and centralized contact-tracing app based on scanning QR codes when people enter various public facilities.[48] Australia[49] also released a voluntary contact-tracing app based on BLE signals and employing the centralized approach.[50]

In the United States,[51] the states of Colorado, Delaware, Florida, Georgia, Hawaii, Indiana, Iowa, Louisiana, Maryland, Missouri, New Mexico, North Carolina, Ohio, Oregon, Tennessee, Texas, and Vermont, as well as cities such as Baltimore and San Francisco, decided not to employ technological means for contact tracing, on the grounds of their inefficiency along with the preference for recruiting additional personnel to do the job.[52] Utah, by contrast, opted for a voluntary contact-tracing app developed by the social network startup Twenty. The app collects BLE signals, cellphone location data, and individuals' contacts, which are stored on the company's server and transmitted the healthcare agencies if a user tests positive for the coronavirus. Rhode Island, South Dakota, Virginia, and Washington state decided to employ contact-tracing apps which are not based on Google's and Apple's exposure notification API. Rhode Island's app collects GPS and BLE signals, Washington's app relies solely on BLE, and South Dakota's app tracks location data. North Dakota, South Carolina, Alabama, and Virginia declared they will utilize a contact-tracing app based on Google's and Apple's exposure notification API.[53]

The Asian democracies, Taiwan and South Korea, fall somewhere between the two extremes of this scale. Taiwan is a relatively new democracy[54] that has amassed recent experience in dealing with pandemics, especially SARS in 2003 and swine flu in 2009. Because of this history, the country has comprehensive legislation that regulates how the authorities deal with a pandemic, authorizes the healthcare service to conduct broad epidemiological studies, and impose sanctions on those who refuse to cooperate with it.[55] When the coronavirus emergency broke out, the immigration and healthcare departments merged their databases, and the combined database made it possible for the government to identify those at high risk for infection and to fine-tune the quarantine directives for them.[56] Cellphone location was used for those ordered into quarantine and for contact tracing. But the identifying data was available exclusively to the head of the Central Pandemic Command Centre. When action against those who violated quarantine orders was required, only the individual's cellphone number was sent to the police. The identifying information transferred to the Central Pandemic Command Centre was deleted after 14 days.[57] From the very start of the campaign, the government was careful to be as transparent as possible, in order to make it clear to the public that despite the emergency situation, the state still maintains its democratic values.[58] The government refused to employ facial recognition technology, and even though it developed a contact-tracing app that makes decentralized use of BLE signals, it decided not to deploy it as long as the outbreak remained under control.[59]

In South Korea[60] — which, like Taiwan, has recent experience in dealing with pandemics — the law permits people to refuse to take part in an epidemiological investigation, but they are subject to sanctions if this refusal cannot be justified.[61] At the same time, the authorities impose strict confidentiality requirements on all information gathered, backed by heavy fines and prison terms for those who violate them.[62] In South Korea, a smart quarantine system collected information about persons who arrived in the country from abroad; there is also extensive monitoring of confirmed patients and of those ordered into quarantine. New arrivals in the country are required to install an app to keep tabs on their medical situation and track their location. Those who violated a quarantine order are issued a geolocation bracelet (if they agree to wear it). The monitoring included cross-checking data on patients' movements against those of anyone who might have been in their proximity, on the basis of cellphone location data received from the cellular providers, credit card firms, surveillance cameras in public areas, satellites, and information from the border control authorities and the airlines.[63]

However, in order to warn those who may have been near a confirmed COVID-19 patient, the South Korean government sent out messages with extensive information about the patient's movements. Even though the information was anonymized, it was relatively simple to do a backward search and identify the patient and his or her habits.[64]

In Israel, the coronavirus pandemic struck at a moment of national weakness in two respects, political and structural. Politically, the country had conducted three national elections in the space of a year and was without a functioning parliament and run by a caretaker government that had not received a public mandate in more than a year. Structurally, Israel lacks up-to-date pandemic-control legislation and privacy protection legislation,[65] and its healthcare system's budget has been starved in recent decades.[66] In addition, there is an inherent tendency of the Israeli system to rely on the security forces — which enjoy ample funding and priority in terms of personnel, knowledge, and technology — to help out in times of emergency.[67]

Section 20 of the Public Health Ordinance, which was enacted by the British mandatory authorities and predates the state, authorizes the minister of health to declare that a disease is contagious, dangerous, and poses a severe threat to public health, and then to issue extremely broad directives in order to prevent or alleviate a pandemic.[68] This includes the quarantining, detention, and surveillance of infected persons and those who come in contact with them. Relying on these powers, the Ministry of Health issued a blanket quarantine order for those who entered Israel from various countries abroad, for citizens who came in contact with confirmed patients, and others.[69]

In addition to these powers, §39(c) of the Basic Law: The Government (with quasi-constitutional power, since Israel does not have a constitution) provides for the declaration of a national state of emergency. When a state of emergency has been declared, the government is empowered to enact emergency regulations that may modify or temporarily suspend the validity of any existing statute. In fact, Israel has been under a state of emergency since independence. Because it has never been revoked, when the coronavirus erupted the government was able to exploit the legal situation in order to approve a number of emergency regulations,[70] which include digital contact monitoring of all Israeli citizens by the General Security Service. The GSS, Israel's domestic secret service, is part of the Prime Minister's Office; in normal times it acts against terrorists and dissidents. It operates in full and total secrecy, pursuant to a law enacted in 2002.[71]

Contact tracing by the GSS relied on cellphone location data, inasmuch as the GSS already had direct access to the cellular infrastructure in Israel. As emerged in retrospect, it routinely collects cellphone location data for all Israeli citizens,[72] but stores them in a pool and makes no use of them in the absence of a court order.

No independent external body exercises oversight of the GSS and monitors its compliance with these restrictions.[73] The GSS Law[74] does not require ex-ante judicial or quasi-judicial review of its activities. An ex-post (or post hoc) review can be carried out only by the attorney general, who does not have access to all of the relevant information and lacks enforcement powers if it turns out that something is amiss. In other words, the oversight exercised by the Knesset Intelligence Committee and by the attorney general is too little, too late.[75] The government claimed that the GSS is the only

> **The oversight exercised by the Knesset Intelligence Committee and by the attorney general is too little, too late.**

entity that has the means to quickly and efficiently identify those who may have been infected by the virus. It added that since Israel had no functioning parliament at the time, there was no alternative to enacting emergency regulations by the government itself. The government stipulated limits on the GSS, such as a ban on transmitting information to any external body other than the healthcare authorities, an obligation to report to the attorney general, and an obligation to delete all information collected when the pandemic is over. It was emphasized that there would be no collection of the content of phone calls or text messages, but only of digital information about location, calls, and text messages.[76]

The emergency regulations gave rise to several petitions to the High Court of Justice,[77] asserting that they were enacted without any parliamentary oversight and infringed on the fundamental constitutional right to privacy in a disproportionate fashion. Already at the first hearing, the justices hinted that they would not allow continued use of the GSS under these emergency regulations.[78] So in a late-night telephone meeting on March 24, the government of Israel decided to repeal the emergency regulations, and instead invoked an unprecedented and extremely broad interpretation of the GSS Law, to be approved by the Knesset Intelligence Committee, in order to authorize the GSS to continue to collect the data. The collection process, the information, its storage, its transmission to the health ministry, and its eventual deletion would be regulated by a confidential procedure to be approved by the attorney general. It was also stipulated that the GSS would not be in direct contact with any patients and would not be involved in monitoring or enforcing quarantine orders. After several meetings, the Knesset Intelligence Committee ratified the use of the GSS in this way.[79]

On April 26, the Supreme Court issued its ruling on the petitions, and held that the government's expanded interpretation of the GSS's powers was illegal. Given the severe infringement of the right to privacy, if the state wished to continue to deploy the GSS in the battle against the coronavirus, it must do so through explicit legislation. On May 4, the government decided to continue to rely on the GSS for contact tracing until June 16, and to sponsor legislation to this effect.[80] Government lawyers went back to the court and declared that there was no alternative to the GSS and that its continued involvement in contract tracing was essential. At the same time, the government began to look into alternate contact-tracing technologies.[81]

Then, on June 8, the Coronavirus Cabinet, an ad-hoc governmental committee composed of the prime minister and 13 ministers, decided to freeze the draft legislation and suspend the health ministry's reliance on the GSS. But the door for its return was left open. [82]

In the meantime, on March 22, the health ministry released a tailor-made contact-tracing app named "Hamagen" (the Shield). Installation is voluntary. The app collects users' cellphone location data and compares it with that of confirmed COVID-19 patients, as found on the health ministry's central server. Users' cellphone location data are stored in the internal memory of their device and uploaded to the health ministry server (the centralized architecture), but only with the user's consent, if he or she is determined to have contracted COVID-19. In the first days after its release, the app was found to be prone to error, due to the imprecision of cellphone location data and human mistakes in the input of information to the health ministry computer system.[83] As a result of these false reports, as well as the absence of an extensive public campaign accompanying its launch to encourage installation of the app, only a small percentage of the Israeli population downloaded it and left it active on their device.[84] In addition, the fact that app cannot be installed on the 600,000 “dumb phones” in the ultra-Orthodox sector left Hamagen as a supplementary tool to traditional human-based contact tracing and to reliance on the GSS.

With the beginning of the second wave of the pandemic in Israel, the GSS was called again to the rescue. The government argued that the use of the GSS’s tool is critical for its ability to fight the pandemic while avoiding draconian lockdown steps. On July 1, a minimized version of a law was enacted, with a limited validity for three weeks. According to this law, the government can use the GSS only when there is clear and present danger of pandemic spread or other exceptional circumstances, or when the number of total COVID-19 cases exceeds 200 on the day the Ministry of Health requests the GSS’s assistance or the day before it. Moreover, using the GSS is only allowed where it is not possible to complete contact tracing using other methods.[85] On July 15, a supplementary bill was introduced that suggests a combined use of a voluntary app in companion with the GSS’s tool.[86] The bill paves the way for constant use of the GSS.

However, so far there is no concrete proof that reliance on the GSS’s tool has been an effective policy that justifies its massive blow to democracy and to human rights in Israel. According to the daily COVID-19 tracking data the Ministry of Health published and the reports it files to the Knesset’s Intelligence Service Subcommittee, on average the GSS’s tool identifies only three in every 10 new COVID-19 cases.[87] Moreover, the Ministry of Health admitted that more than 12,000 citizens — out of the 70,949 it has ordered to get into quarantine based on the GSS’s tool — were mistakenly identified, which means it has a false positive rate of 16 to 20%.[88]

FIGURE 1: SUMMARY OF THE COMPARISON BETWEEN ISRAEL AND OTHER COUNTRIES

Country	Freedom House Global Freedom Score	Legislation for epidemics (excluding special laws or orders triggered by the COVID-19 pandemic)	Privacy legislation	Technology
China	10, not free			Centralized mandatory mass surveillance, facial recognition, and social scoring
Israel	76, free	Public Health Ordinance, 1940	Protection of Privacy Law, 5741-1981	Centralized mandatory mass surveillance GPS-based, by the GSS; oversight by the Knesset and Supreme Court

Taiwan	93, free	Communication Disease Control Act 2004	Personal Data Protection Act 1995	Centralized, transparent, civilian-run (by health authorities) but mandatory mass surveillance; GPS-based
South Korea	83, free	Infection Disease Control and Prevention Act amended in 2015 following the Middle East Respiratory Syndrome (MERS) outbreak	Personal Information Protection Act 2016, the Act of the Promotion of Information and Communication Network Utilization and Information Protection 2016	Centralized, transparent, civilian-run (by health authorities), but mandatory mass surveillance GPS-based; cross-checking of data from the immigration authorities, airlines, credit card companies, and surveillance cameras in public areas
New Zealand	97, free	Civil Defense Emergency Management Act 2002, Epidemic Preparedness Act 2006	Privacy Act 1993	Centralized voluntary app; QR code-based As part of the reopening of the economy, a new centralized but voluntary contact-tracing app based on scanning QR codes at the entrances of public places
Australia	97, free	Public Health Act 1997	The Privacy Act 1988	Voluntary app; BLE-based; centralized
France	90, free		GDPR	Voluntary app; BLE-based; centralized
United Kingdom	94, free	Public Health (Control of Disease Act 1984), the Civil Contingencies Act 2004	The Data Protection Act 2018	Voluntary app; BLE-based; decentralized
Switzerland	96, free	Epidemics Act 2016	Data Protection Act 1992	Voluntary app; BLE-based; decentralized
Germany	94, free	Protection Against Infection Act 2000	GDPR	Voluntary app; BLE-based; decentralized
Austria	93, free	Epidemics Act 1950	GDPR	Voluntary app; BLE-based; decentralized
Italy	89, free	Consolidated Health Laws	GDPR	Voluntary app; BLE-based; decentralized

The main differences among various countries can be summarized as follows:

- All the countries studied employed various data-collection and tracking technologies to deal with the pandemic.
- Some European countries, Australia, New Zealand, and the Asian democracies have specific, up-to-date legislation for dealing with pandemics, which also relate to methods of digital data collection during the crisis. In Israel, the relevant legislation is very old (1940)[89] and obviously has nothing to say about digital data collection.
- The European countries, Australia, New Zealand, and the Asian democracies have up-to-date privacy protection legislation; the Asian democracies are in the process of modifying theirs in order to receive the European Commission acknowledgement of their adequacy under the European GDPR.[90] The privacy protection legislation in Israel is out of date, but efforts are being made to achieve adequacy with the GDPR.
- Cellphone location data is used to track specific individuals and conduct epidemiological studies or enforce quarantine orders in Asian countries and in Israel, but not in most European countries[91] or in the United States. The Asian democracies do this by virtue of existing legislation that permits tracking. In Israel, it required emergency legislation and later on a specific law.
- Of all the countries we looked at, only in China and Israel were the intelligence agencies involved in the collection of tracking data. The cellular providers and other companies transmit cellphone data directly to the healthcare authorities who deal with the coronavirus pandemic and not via the intelligence agencies or security organizations.
- In all the democracies we studied, digital contact tracing is carried out exclusively by means of the voluntary installation of Bluetooth-based applications (except for New Zealand, which uses a contact-tracing app based on QR codes). The disagreements relate to where the anonymized data is decoded and processed in order to identify those who spent time in physical proximity to confirmed COVID-19 patients, so that the person can be quarantined. Supporters of the decentralized approach prefer that the decoding and decision as to whether a person must enter quarantine is on his or her own cellular device; those who favor the centralized approach want to leave the control of decoding and contact tracing to the national authorities, so that they can produce an up-to-date picture of the extent of the virus's spread and monitor compliance with quarantine orders.[92]
- Taiwan and South Korea, whose approach is more invasive of privacy, minimized the infringement of other fundamental freedoms, notably freedom of movement. The insistence on transparency in Taiwan and South Korea stood out.

WHERE ISRAEL SITS ON THE SCALE

The Israeli decision to deploy the GSS to conduct digital contact tracing was an extreme and unprecedented move. The GSS has never been used for domestic surveillance on such a scale. Unfortunately, the decisionmakers viewed this infringement of the constitutional right to privacy as marginal and justified. Even if they were apprehensive about granting such powers to the GSS, the greater fear was of harm to the GSS itself because of the change in its operational genome and the possibility that it be compelled to make some of its operating methods public. Even when the COVID-19 curve of infection was flattened in May, with an average of 38 new COVID-19 cases per day,[93] and the economy began to return to normal, the government was unwilling to stop using the GSS and announced its intention to amend the current GSS law in order to permit its continued use for contact tracing.[94]

The Coronavirus Cabinet decided, on June 8, to freeze the draft legislation and suspend the health ministry's reliance on the GSS. But it was only a temporary break.[95] With the increase in COVID-19 new cases per day, the bill was re-introduced as a temporary law for three weeks,[96] and a broader bill was passed in the Knesset two weeks later.[97]

> **Israel effectively positioned itself on the scale between the Asian democracies and China, an extremely problematic place, and far from all of the democracies we examined.**

On the scale presented above, Israel is very far from the approach of the GDPR countries and Australia, New Zealand, and the United States, which from the very start stipulated that centralized involuntary data collection is illegal, even in a state of emergency. It even went a step beyond the Asian democracies, such as South Korea and Taiwan, with their centralized involuntary collection of cellphone location data — but those countries did not involve their security forces, secret services, and law enforcement agencies (rather, the information collected passed directly from the telecommunication companies to the healthcare authorities). Israel effectively positioned itself on the scale between the Asian democracies and China, an extremely problematic place, and far from all of the democracies we examined. This is an uncomfortable and troubling conclusion for Israeli citizens, who find themselves exposed to a very broad infringement of their rights, perhaps the broadest since the birth of the state. We may assume that it will also influence Israel's ranking on international democracy indexes, as well as perhaps influence the European Commission's decision as it considers whether Israel's privacy legislation is comparable to the European privacy legislation and hence should be declared again as adequate under the GDPR.[98]

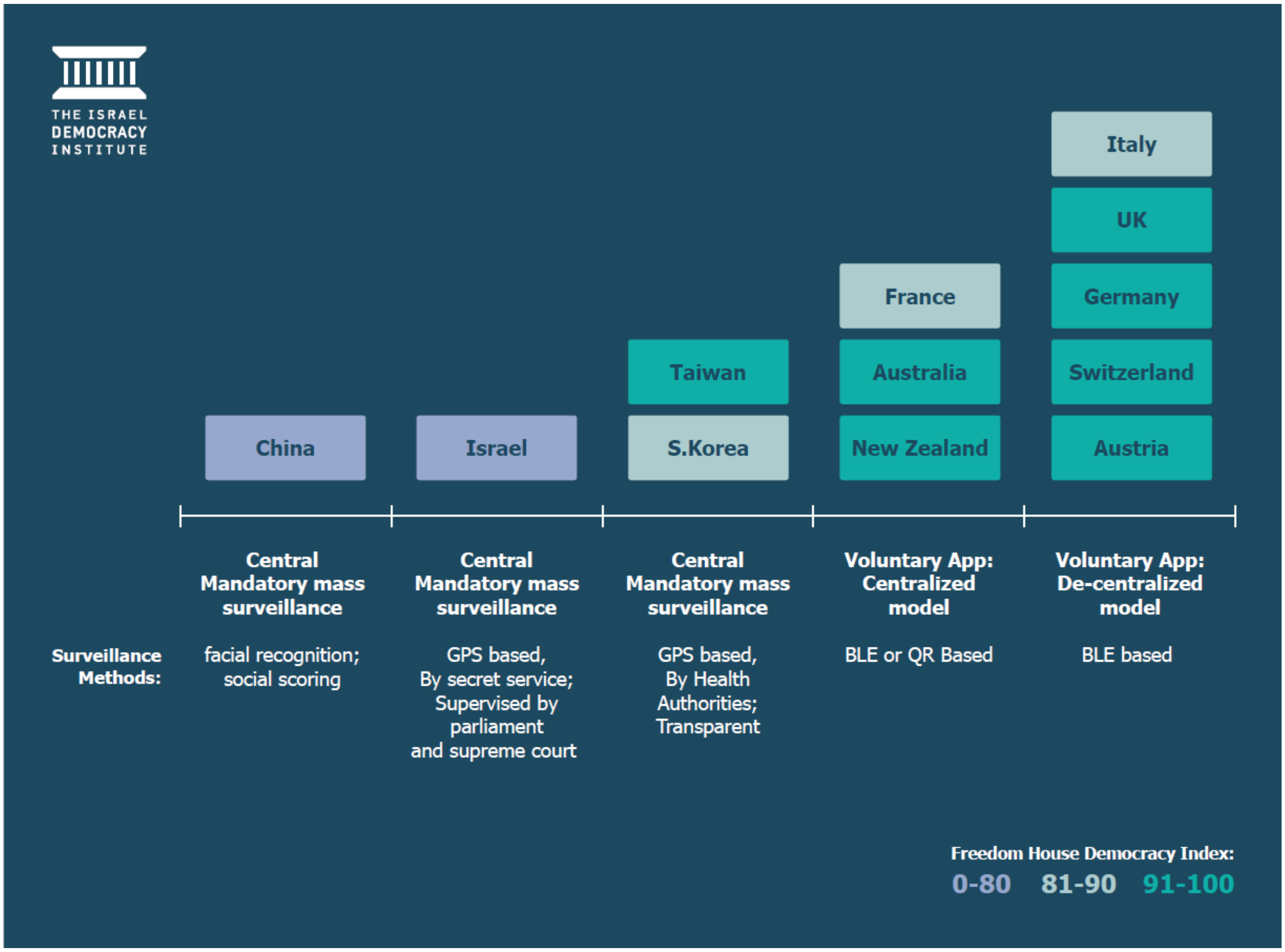
In fact, the coronavirus pandemic is not only a biological incident, but also a political event that reflects the relationship between the country and its citizens, and that interacts with human behavior, social institutions, a culture of obedience, and a history of confidence in the government. It is precisely for this reason that the Israeli case is complex, as we will now show in greater detail.

The strength of its democracy does not seem to guarantee a country's effective response to the pandemic

For various reasons, including due to the quarantine on all those entering the country and lockdowns imposed at a relatively early stage of the pandemic, Israel has been able (at least so far) to avoid a tragedy of historic proportions with regard to morbidity and mortality rates. "Our success is not based on genetics or climate," declared Prime Minister Benjamin Netanyahu in a speech about Israel's impressive achievements in its fight against the coronavirus. He added: "The success is based on three basic things: first of all, the quick and carefully planned steps we took at the beginning of the worldwide crisis — sealing the borders, home quarantine, and digital tracking.[99] What is more, Israel did not adopt a neoliberal policy — giving precedence to avoiding economic damage and protecting the interests of the powerful — but took drastic steps aimed at protecting grandma and grandpa.[100] For Israeli leadership, the general public welfare and the social compact between the state and its citizens, so as to maximize the common good, justified the grave blow to individual rights.

Similarly, the Asian democracies that took an instrumental attitude towards the involuntary collection of private data dealt with the pandemic successfully. Taiwan and South Korea used cellphone location data to identify chains of contagion, order people into quarantine, and enable the healthcare system to gear up for the next wave of infection. They also cross-checked cellphone location data against databases on people's age, medical history, and travel abroad, in order to identify super-spreaders. New Zealand, which is a strong democracy, depended on widespread lockdowns and social distance measures, but implemented a voluntary and centralized contact tracing app, based on scanning QR codes, only when it reopened the economy.[101] By contrast, the United States, which is also a strong democracy, as well as European countries subject to the GDPR, failed miserably, as judged by the public health results.

FIGURE 2: SELECT COUNTRIES' COVID-19 DIGITAL CONTACT-TRACING MODELS


THE ISRAEL DEMOCRACY INSTITUTE
Italy
UK
France
Germany
Taiwan
Australia
Switzerland
China
Israel
S.Korea
New Zealand
Austria
Central Mandatory mass surveillance
Central Mandatory mass surveillance
Central Mandatory mass surveillance
Voluntary App: Centralized model
Voluntary App: De-centralized model
Surveillance Methods:
facial recognition; social scoring
GPS based, By secret service; Supervised by parliament and supreme court
GPS based, By Health Authorities; Transparent
BLE or QR Based
BLE based
Freedom House Democracy Index:
0-80
81-90
91-100

The crisis was turned into a matter of national security

To no one's surprise, Israel was revealed to be a country in which problems that affect society, economy, and government are translated into issues of national security.[102] This was evident both in the rhetoric of the campaign against the coronavirus, as if it were some type of human enemy, and in the reliance on the Israeli defense and security establishment for support in many areas:[103] the provision of services (running hostels for COVID-19 patients, supplying food to neighborhoods under lockdown, running public relations and public information campaigns); R&D projects for developing better contact tracing technology and in search for vaccines; delegating the intelligence agency Mossad to purchase medical equipment abroad; and more.

Furthermore, a well-known Israeli cliché has it that "Israel isn't a country that has an army, but an army that has a country." During an emergency, it is only logical to rely on the military forces, which are well-fed in normal times, whereas those that survive on lean budgets, such as the healthcare system, are apt to collapse. In the end, it's all Israeli taxpayer money.

In addition to the organizational culture of dependence on the security establishment, Israelis express very high confidence in it, surpassing their trust in any other institution (including the Supreme Court, the Knesset, the government, the police, political parties, and the media). This is a long-standing phenomenon corroborated by the findings of the Israel Democracy Index survey, which the Israel Democracy Institute conducts annually.[104] According to a special survey conducted in late March 2020, 51% of the public believes that management of the coronavirus crisis should remain with the health ministry, while the other half of the population think it justified to transfer this responsibility to the Ministry of Defense and Israel Defense Forces (IDF).[105]

Even though public trust in the secret services is not assessed in the annual Democracy Index survey, it is likely that Israelis see the GSS as a branch of the armed forces. In fact, in another survey conducted in late March 2020, 63% of the Jewish public in Israel and 38% of the Arabs responded that they rely on the GSS to make responsible use of the data collected for the purpose of contact tracing.

Taking into account the broader context, the reliance on the GSS and its surveillance systems seemed to be perfectly understandable during the first wave. However, in our opinion, enlisting the security agencies to carry out activities that are not exactly humanitarian in nature, but are intrusive military policing actions — such as sending troops to accompany police units to enforce quarantines and lockdown orders, or to collect information about the civilian population — broadcasts a troubling message. First of all, with regard to the population, the practical implication is that technology or other capacities intended for use against an enemy may ultimately be deployed against citizens as well. Second, even if security agency personnel have been taught to think that their unrestricted activities (exceeding both physical, legal, and moral limits) are justified in a war against an enemy, now they are being asked to wield them against Israeli citizens — more precisely, against their own family and friends.

The democratic system still has checks and balances.

Israel is not the only country that took advantage of the coronavirus emergency to infringe on human rights. Countries such as China and Russia saw the pandemic as a golden opportunity to expand the state's coercive powers over citizens and to use technology in order to identify, track, acquire knowledge, and intimidate. When the pandemic dies down, they will find some other excuse, and the heightened surveillance will continue. In Israel, too, the decisionmakers' obstinate insistence on continued use of the GSS and rejection of alternatives corroborate the claims about the slippery slope whose bottom is unpredictable. In addition, Israel finds itself in the company of illiberal democracies such as Poland, Turkey, Bulgaria, and Hungary, which exploited the coronavirus in order to strip people of their civil rights and to ignore their parliaments and courts. The number of emergency regulations enacted by the government of Israel from March to June exceeds the figure for any period in the past, including in the most serious emergencies the country has known.[106] They dealt a severe blow to citizens' rights and to the regulation of extensive areas of economic and civilian activity, with contact tracing being only one of them.

What is more, Israel's problematic political situation at the start of the crisis — three hung elections over the course of a year, a newly elected parliament that had not yet convened for the first time, no elected government, and Prime Minister Netanyahu's trial on corruption charges scheduled to begin in mid-March[107] — added to fears around the sweeping use of emergency powers. Moreover, there was a heightened suspicion that the prime minister had a conflict of interest, both because of the pressure he exerted on coalition partners to join him to cope with the emergency, and because of his desire to postpone the start of his trial. Many saw the use of the GSS for mass surveillance as an attempt to over-dramatize the situation, in pursuit of the prime minister's other goals.

On the other hand, taken as a whole, the digital contact tracing case reveals that Israel does have a functioning system of checks and balances. Civil society spoke out loudly and kept the issue on the public agenda. Appeals to Knesset members and High Court petitions led to significant curtailment of the original government decisions. The Knesset Foreign Affairs and Defense Committee held hearings and demanded a greater degree of transparency than the government had planned on.[108] The High Court ruled that the GSS could not be given such sweeping powers purely on the basis of a government decision, and twice ordered the government to obtain parliamentary approval for its policies.[109]

What is more, and somewhat paradoxically, the coronavirus emergency ultimately generated political stability and facilitated the establishment of an elected government and functioning parliament, after a year of paralysis. The absence of checks and balances was manifested mainly against pressure groups in the Israeli political system, first and foremost the ultra-Orthodox. It was not demonstrated against the court or parliament. In part, it was because most members of the ultra-Orthodox sector do not use smartphones that the government opted for mass involuntary contact tracing by the GSS, rather than the voluntary installation of cellphone applications.[110]

The role of trust and compliance versus coercion

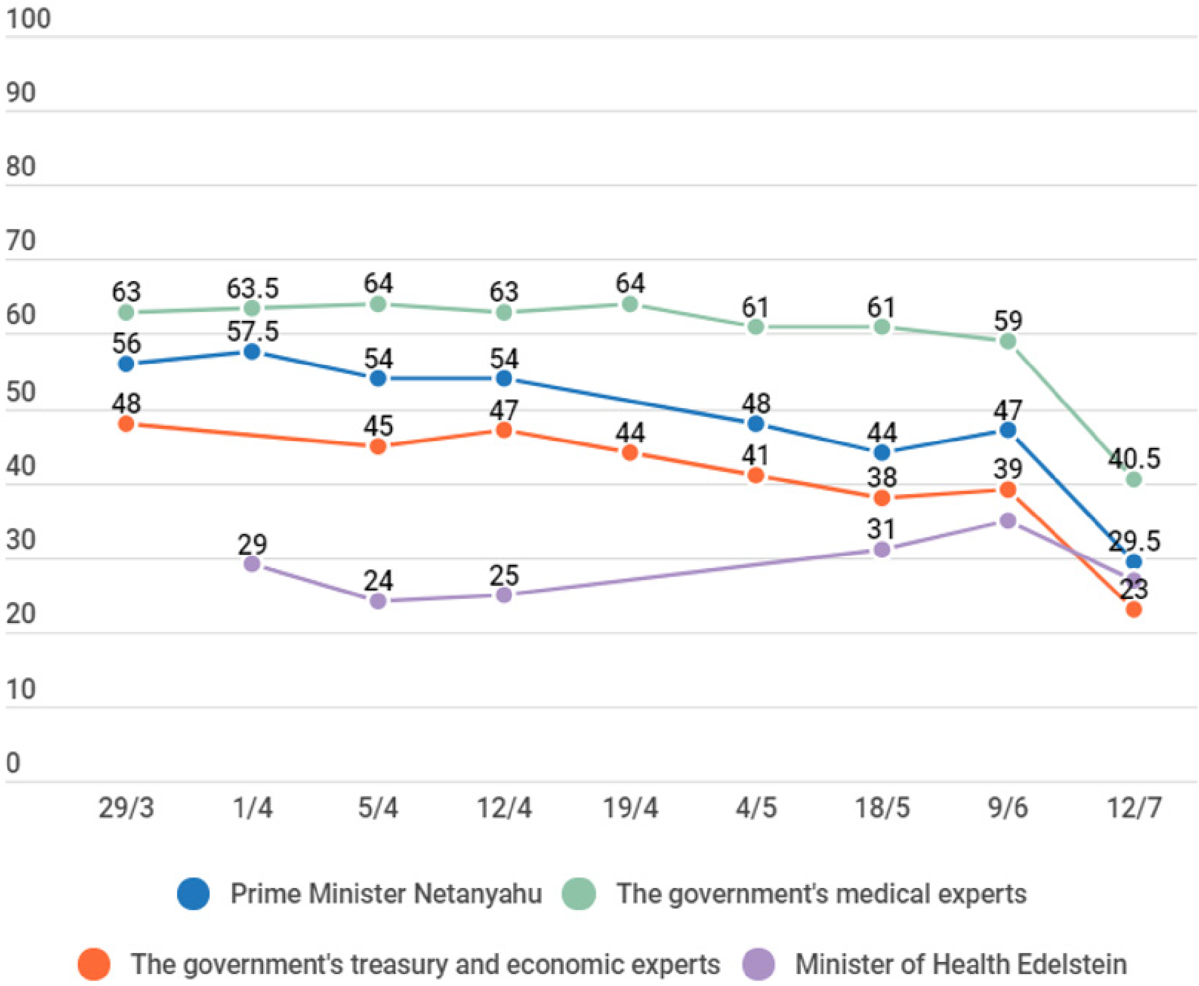
Strong democracies like Sweden, the Netherlands, and Germany elected to base their response to the crisis on the population's sense of civic commitment. They could assume that their citizens' self-discipline would make them show concern for themselves and for others, and in effect forged trusting relations with the people. The Asian democracies went for transparency, open communication, and accountability, combined with a strong social safety net, which was crucial for creating the public trust required for the strict monitoring methods they employed.[111] The Israeli management of the crisis was essentially one of command and control. The government enacted regulations instead of relying on the public's self-discipline and preferred a compulsory system of monitoring and enforcement by the GSS, the police, and the military. There was no transparency about decision making processes, and the information required to critique them was not made accessible. The reliance on the GSS, a top-secret agency by definition, meant that the procedures and regulations for the technologies used were not transparent to the public; the same applies to the parliamentary discussions about them. In recent weeks, the working paper drafted by the National Security Council to examine alternatives to the use of the GSS has also remained under wraps.

On the surface, conditions were ripe for public unrest and skepticism. However, the reliance on the GSS does not seem to have reduced citizens' confidence in the government or willingness to comply with draconian rules.

The explanation for this lies in the complexity of the relations between the authorities and citizens in Israel. The regime has many different entities. Public confidence in them was uneven before the pandemic, so the response to their instructions and faith in their good judgment was not uniform. Israelis tend to trust the military and other security agencies,[112] and this may explain the relative equanimity with which they accepted the decision to conduct widespread tracking. On the other hand, Israeli citizens have less confidence in the education system, so when the schools reopened, many parents chose not to send their children back to the classroom.[113]

With the beginning of the second wave of the pandemic and the re-authorization of the use of the GSS under the law,[114] 70,949 people received text messages from the Ministry of Health notifying them that they have been in contact with a person with coronavirus and thus have to self-isolate. Of them, 70,051 were identified solely by the GSS.[115] Many people thought their identification as being in contact with a person with coronavirus was a mistake. However, it was difficult and even impossible to appeal the isolation directive. The Ministry of Health Hotline has been receiving many phone calls and collapsed. Many people waited for a very long time, and some phone calls got disconnected.[116] The media discussed this matter intensively and there was a growing acknowledgement that the GSS's tool is not as efficient as it was claimed to be.[117] Still, the general public did not criticize the use of the GSS's tool itself. Rather, public dismay focused mainly on the large percentages of mistakes in the identification of people who were in contact with a person with coronavirus, and the Ministry of Health was perceived as responsible for that. Public anger was directed to the Ministry of Health's failure to process all the isolation appeals and the collapse of its hotline.[118] Therefore, an additional survey conducted by the Israel Democracy Institute in mid July 2020, while Israel is experiencing a "second wave" of the pandemic, revealed a collapse in public confidence in both the prime minister and the health authorities.[119]

FIGURE 3: TRUST IN THE INDIVIDUALS AND GOVERNMENT PROFESSIONALS LEADING ISRAEL'S FIGHT AGAINST THE CORONAVIRUS (%, GENERAL PUBLIC)



Source: Israel Democracy Institute[120]

We must also take account of the culture of obedience.[121] In countries with a strong tradition of ignoring government instructions, such as Italy, leaving citizens to make the decision about entering quarantine and sharing information seems to have directly contributed to the scale of the disaster.[122] It is possible that in Germany, for example, with its stricter culture of compliance, it is easier to get people to use tracking applications. Israeli society is less compliant, so one may wonder whether a wholly voluntary model would work here.

RECOMMENDATIONS

The fact that the coronavirus pandemic erupted so surprisingly required many countries to make rapid, on-the-fly decisions of principle and practice about the balance between public health and the right to privacy. Technological advances, such as the creation of cellphone apps, also took time. In the interim, from a global perspective, the first serious wave of contagion seems to have passed. But the fear of future waves, including a combination of influenza and a COVID-19 outbreak in the coming winter, as well as the lessons we have learned that can be applied to possible future pandemics, requires that we draw conclusions and make recommendations.

Based on our comparative survey and the Israeli experience, we believe that exclusive reliance on voluntary cellphone apps cannot provide an adequate solution for digital contact tracing, should there be a new outbreak of the pandemic, despite the clear advantages of such apps for the protection of privacy. There are two reasons for this. First, if we are talking about apps based on the decentralized architecture described above, the healthcare services lack the capacity to conduct sufficient centralized tracking of a chain of contagion and of morbidity as a result of infection.[123] The second reason is the fear that not enough people would install these apps on their phones, so it would be impossible to rely exclusively on this means for broad and effective contact tracing. The experience in Singapore and Israel supports this concern.[124]

Given these disadvantages, we can envisage one of the following scenarios when the virus strikes again:

1. Minimal or no use of technology for contact tracing, even though such technology exists and can be helpful. There may be attempts to deal with the pandemic in other ways, such as extensive random checks of the population, with the downside being that they cannot be relied on if there is a shortage of test kits; or human epidemiological studies, which have many disadvantages, including their lack of scalability, people's imperfect memories, and the inability to determine who was close to super-spreaders (such as on trains). There is also the practical difficulty of publicizing confirmed patients' contact history and reaching those who should be going into quarantine, as well as the fear that people whose contact history is published could be reverse-identified, even if their names are omitted. In any case, in this scenario, a significant technological advantage for dealing with the pandemic is lost.

2. Replacement of voluntary apps with extensive involuntary digital contact tracing. This could include centralized data collection from cellular providers and deploying security agencies and secret services that regularly engage in such activities against enemies, terrorists, or dissidents. The justification for this, of course, would be saving lives, relying on the fact that even if the app-based method fails, there are good reasons to continue with digital contact tracing, and it is appropriate to employ any available technology to do this. This scenario could turn democratic countries, especially weaker democracies that — unlike Israel — do not have a strong system of checks and balances, into surveillance dictatorships.

We propose a middle way between the first and second scenarios, focusing on the search for solutions to the problems associated with the use of cellphone apps, even if some of these solutions lead to a greater infringement of privacy than does the voluntary reliance on decentralized apps. With this in mind, it is necessary to draw up a plan for a broad and active campaign to encourage installation of the apps and to prefer the centralized approach that requires users testing positive for the coronavirus to transmit the contact history stored on their cellphone to the central server of the health services.

Our recommendations are as follows:

- **The purpose of tracking must be strictly limited.** Tracking intended to identify contacts must be limited exclusively to the need to inform those exposed to a confirmed COVID-19 patient that they must enter quarantine. General analyses to support policymaking (such as drawing maps of contagion hotspots, presenting data graphically, forecasting, and developing advance preparation systems) should be based on aggregate data only (or at least on anonymized data). Comprehensive analyses to determine policy that are based on identifying individual information must be rejected as disproportionate.

- **Agencies that have enforcement and investigative powers should not be permitted to engage in contact-tracing activity.** There are essential differences between civilian agencies that collect information, such as the healthcare system, and organizations that collect information but also have investigative or enforcement powers. These differences relate to how they operate the limits on their powers, and the bounds of their responsibility. Entities of the second type should not be permitted to collect data.

- **Any infringement of privacy must require the individual's consent.** The fact that this is a civilian crisis, the severity of the infringement of human rights, the breathing room we now enjoy because the pandemic is easing, and the need to achieve citizens' trust mean that installing cellphone apps must be voluntary, rather than compulsory for centralized data collection.

- **People must be encouraged to install apps on their cellphones.** Substantial advertising and public information campaigns are required to encourage people to install these apps, similar to that employed in Australia when the government launched its campaign to encourage citizens to install the COVIDSafe app.[125] Some of this publicity effort must be based on empowering users: They need to receive an explanation of why to use of the app and of the moral context of helping other people, how the app works, and what privacy protection are incorporated in it. Concepts from behavioral economics should be utilized to increase the app's penetration among cellphone users. For example, those who install it could be given priority for certain public services (assistance grants, or various permits and certificates) or offered material benefits (coupons or discounts). The opt-out model, in which the app is installed by default on all cellular devices but users have the option of removing it, should be adopted.[126] Certain sectors of the population or residents of specific regions in which there is a high incidence of coronavirus infections should be required to install the app. Indirect means to encourage the installation of the app can be applied, such as by making the use of public transportation conditional on its installation, or requiring shop owners to verify that customers entering their store have done so. As we see it, this method is far preferable than requiring people to identify themselves before they can enter stores and shopping malls, as has been proposed in various places. Employers should be required to verify that their workers have installed the app as a condition for coming back to work. This system would avert a situation in which employers collect unneeded information about workers or decide to develop their own apps and require workers to install them.

- **Solutions must be found for those who do not own smartphones.** Those who do not own smartphones or do not wish to install the app should be allowed to use a smartcard, the size of a credit card, which operates in similar fashion as the app (this has been proposed in New Zealand).[127]

- **Transparency and trust are important.** When information is transmitted to a central computer controlled by the state, which also has the keys for decoding the information, there is a fear that individuals could be reverse-identified and exposed. For example, linking to the IP address of an individual's cellular device makes it possible to determine the owner's home address and identity. The state, or commercial entities that get access, could misuse the information.[128] So even if the use of tracking technologies is justified and imperative, it must be accompanied by effective parliamentary, administrative, and judicial oversight to verify that the conditions for data collection, processing, use, and security are respected. Reporting and transparency provisions — what information is collected, for what purpose, and when it will be deleted — must be imposed. There must also be a way to appeal orders to enter quarantine.

CONCLUSION

The coronavirus pandemic caught the world at a historic moment of tracking and monitoring technologies with impressive capabilities. When lives are at stake, it is logical and even imperative to make use of every available technology. The question, as in other contexts of life, is one of proportion. Who tracks, who is tracked, what information is collected, and who supervises all of this?

Personal information is power. Governments and private entities that possess extensive information about large swaths of the population have vast power to control, engineer, and influence. History teaches us that extreme and extraordinary events can generate quantum leaps in the efforts to amass information and engage in mass surveillance. In the United States, the 9/11 attacks turned the internet and telecommunication networks into the largest espionage enterprise in history. The Summer Olympic games in Beijing in 2008 were the occasion for a further tightening of the surveillance noose on the Chinese population. Today, with the coronavirus pandemic, China has gone even further, not just tracking telephones but also using facial recognition systems. The fear is that there will be no retreat from the new level of surveillance after the trigger event has passed, and that closer surveillance will remain with us. In addition, every such leap creates a new technological ecosystem that proposes ideas, products, and technologies to make them possible.[129]

The bottom line is that the methods that each country comes to perceive as acceptable, reasonable, and inevitable, will be with us forever. The Israeli experience shows that the road to mass surveillance by the intelligence service is not a very long one, even where meaningful checks and balances exist. So that other democracies, too, can stop before they reach this point in reaction to future pandemics — and in order to avoid falling down a slippery slope later on — we must work today to draft new policies and plans that recognize the need for compromising on some aspects of the right to privacy.

REFERENCES

[1] See, e.g., Jan H. Blits, “Hobbesian Fear,” *Political Theory* 17, no. 3 (August 1989): 417, https://doi.org/10.1177/0090591789017003003

[2] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser, “Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing,” *Science* 368, no. 6491 (March 2020), https://doi.org/10.1126/science.abb6936; Marcello Lenca and Effy Vayena, “On the Responsible Use of Digital Data to Tackle the COVID-19 Pandemic,” *Nature Medicine* 26 (March 2020): 463-464, https://doi.org/10.1038/s41591-020-0832-5; Richard Mark Kirkner, “Contact Tracing, Isolation Have Impact, Study Shows,” The Hospitalist (April 29, 2020), https://www.the-hospitalist.org/hospitalist/article/221446/coronavirus-updates/contact-tracing-isolation-have-impact-study-shows; Tyler M. Yasaka, Brandon M. Lehrich, and Ronald Sahyouni, “Peer-to-Peer Contact Tracing: Development of a Privacy-Preserving Smartphone App,” *JMIR Mhealth Uhealth* 8, no. 4 (April 2020), https://mhealth.jmir.org/2020/4/e18936/; Jeffrey P. Kahn et al., *Digital Contact Tracing for Pandemic Response, Ethics and Governance Guidance* (Johns Hopkins University Press, 2020),

[3] Sangchul Park, Gina Jeehyun Choi and Haksoo Ko, “Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea – Privacy Controversies,” *JAMA* 323, no. 21 (April 23, 2020): 2129-2130, doi.org/10.1001/jama.2020.6602.

[4] Andy Greenberg, “Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered,” Wired, April 17, 2020, https://www.wired.com/story/apple-google-contact-tracing-strengths-weaknesses/; Ramsey Faragher, “The Hidden Trade-Offs Inside Contact-Tracing Apps,” *Forbes*, April 21, 2020, https://www.forbes.com/sites/ramseyfaragher/2020/04/21/the-hidden-trade-offs-inside-contact-tracing-apps/#5fbbda81ea07; Mike Wright and Jack Hardy, “NHS Contact Tracing App Could Give Out False Alerts as Bluetooth Goes Through Walls,” *The Telegraph*, May 2, 2020, https://www.telegraph.co.uk/news/2020/05/02/nhs-contact-tracing-app-could-give-false-alerts-bluetooth-goes/; Patrick Howell O’Neill, “Bluetooth Contact Tracing Needs Bigger, Better Data,” *MIT Technology Review*, April 22, 2020, https://www.technologyreview.com/2020/04/22/1000353/bluetooth-contact-tracing-needs-bigger-better-data/.

[5] Today close contact is defined as being within approximately 2 meters (6 feet) of a COVID-19 patient for more than 15 minutes.

[6] This was also the recommendation of the European Commission. See: “Communication from the Commission, Guidance on Apps Supporting the Fights Against COVID 19 Pandemic in Relation to Data Protection,” European Commission, April 17, 2020, (2020/C 124/I/01), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29.

[7] Zack Whittaker, “A Passwordless Server Run by Spyware Maker NSO Sparks Contract-Tracing Privacy Concerns,” *TechCrunch*, May 7, 2020, https://techcrunch.com/2020/05/07/nso-group-fleming-contact-tracing/.

[8] Paul Lewis, David Conn and David Pegg, “UK Government Using Confidential Patient Data in Coronavirus Response,” *The Guardian*, April 12, 2020, https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response.

[9] Nevertheless, it is important to note that pursuant to the Government decision to empower the GSS to conduct digital contact tracing, the GSS does not collect the content of calls, but only “communication data of identification, location, and contact data.” See: “Government Resolution 4950,” Government of Israel, March 31, 2020, https://www.gov.il/he/departments/policies/dec4950_2020, §13, 17–18.

[10] An app based on BLE signals estimates the physical proximity by means of the transmission of random ID codes at fixed short time intervals over BLE signals. Every telephone device on which the app is installed receives and stores a “signal log” of all the ID codes transmitted in its vicinity by other devices, along with a timestamp and the strength of the Bluetooth signal received, in order to estimate the physical distance between the devices. The determination as to whether a user was exposed to a confirmed COVID-19 patient is based on a comparison of the ID codes stored on an individual’s device with those stored on the patient’s cellular device and a check as to whether identical ID codes were received in sequence, in order to verify that the physical proximity did indeed exceed the period defined by the epidemiological indicators. If the data coincide, the implication is that the COVID-19 patient and the user were near to each other and that the user should go into quarantine. See, e.g., Andy Greenberg, “Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered.”

[11] The Hamagen app in Israel, TraceTogether in Singapore, COVIDSafe in Australia, StopCovid in France, the NHS CV19 in Britain, and Aarogya Setu used by the Indian government, are based on centralized architecture. The contact tracing app used in Germany, the Italian Immuni, and DP-3T, used by the governments of Switzerland and Austria, employ the decentralized approach. For a review of the current contact-tracing apps, see: Patrick Howell O’Neill, Tate Ryan-Mosley and Bobbie Johnson, “A Flood of Coronavirus Apps Are Tracking Us. Now It’s Time to Keep Track of Them,” *MIT Technology Review*, May 7, 2020, https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/. See also Tehilla Shwartz Altshuler and Rachel Aridor Hershkovitz, “Tracking Citizens: What is Going On in the World?” [in Hebrew], The Parliament 84, March 25, 2020, https://www.idi.org.il/parliaments/30997/31088.

[12] “Privacy-Preserving Contact Tracing,” Apple and Google, May 2020, https://www.apple.com/covid19/contacttracing.

[13] Natash Lomas, “Germany Ditches Centralized Approach to App for COVID-19 Contacts Tracing,” TechCrunch, April 28, 2020, https://techcrunch.com/2020/04/27/germany-ditches-centralized-approach-to-app-for-covid-19-contacts-tracing/; Leila Abboud, Joe Miller and Javier Espinoza, “How Europe Splintered Over Contact Tracing Apps,” *Financial Times*, May 10, 2020, https://www.ft.com/content/7416269b-0477-4a29-815d-7e4ee8100c10; Fred Vogelstein and Will Knight, “Health Officials Say ‘No Thanks’ to Contact-Tracing Tech,” *Wired*, May 8, 2020, https://www.wired.com/story/health-officials-no-thanks-contact-tracing-tech/; Jack Kelly, “Contact Tracing: A Newly Created ‘Big Brother’ Bureaucracy Tracks Down COVID-19 – Infected People And Those Who Have Been In Contact With Them,” *Forbes*, May 12, 2020, https://www.forbes.com/sites/jackkelly/2020/05/12/contact-tracing-a-newly-created-big-brother-bureaucracy-tracks-down-covid-19-infected-people-and-those-who-have-been-in-contact-with-them/#19af556e5c42.

[14] Dephne Leprince-Ringuet, “Contact tracing: France snubs Apple and Google but its StopCovid app still underwhelms,” ZDNet, June 29, 2020, https://www.zdnet.com/article/contact-tracing-france-snubs-apple-and-google-but-its-stopcovid-app-underwhelms/; Hariz Baharudin, “Apple-Google’s contact tracing system not effective for Singapore,” *The Straits Times*, June 16, 2020, https://www.straitstimes.com/singapore/apple-googles-contact-tracing-system-not-effective-for-spore-vivian; Ben Grubb, “‘There is no way we’re shifting’: Australia rules out Apple-Google coronavirus tracing method,” *The Sydney Morning Herald*, June 29, 2020, https://www.smh.com.au/technology/there-s-no-way-we-re-shifting-australia-rules-out-apple-google-coronavirus-tracing-method-20200629-p5573s.html9.

[15] Zak Doffman, “Yes, Apple And Google Have Given Us A Serious Contact Tracing Problem – Here’s Why,” *Forbes*, June 19, 2020, https://www.forbes.com/sites/zakdoffman/2020/06/19/how-apple-and-google-created-this-contact-tracing-disaster/#2ca4470e7ca2; Greig Paul, “Contact-tracing apps: Apple dictating policies to nations won’t help its EU anti-trust probe,” The Conversation, June 25, 2020, https://theconversation.com/contact-tracing-apps-apple-dictating-policies-to-nations-wont-help-its-eu-anti-trust-probe-141304.

[16] Mandy Lee, “Given low adoption rate of TraceTogether, experts suggest merging with SafeEntry or other apps,” Today, May 8, 2020, https://www.todayonline.com/singapore/given-low-adoption-rate-tracetogether-experts-suggest-merging-safeentry-or-other-apps; “Singapore hands out coronavirus tracing devices,” BBC News, June 29, 2020, https://www.bbc.com/news/business-53216450; Mark Jones, “Are Wearables the answer to contact tracing app problems?,” TechWireAsia, June 8, 2020, https://techwireasia.com/2020/06/are-wearables-the-answer-to-contact-tracing-app-problems/.

[17] Charlotte Jee, “8 million people, 14 alerts: why some covid-19 apps are staying silent,” *MIT Technology Review*, July 10, 2020, https://www.technologyreview.com/2020/07/10/1005027/8-million-people-14-alerts-why-some-covid-19-apps-are-staying-silent/; Ariel Bogle, “COVIDSafe app tests revealed iPhone performance issues at launch that weren’t shared with the public,” ABCNews, June 16, 2020, https://www.abc.net.au/news/science/2020-06-17/covidsafe-contact-tracing-app-test-documents-rated-poor-iphone/12359250.

[18] “New Zealand to roll out ‘digital diary’ app to help people track movements,” Reuters, May 18, 2020, https://www.reuters.com/article/us-health-coronavirus-new-zealand/new-zealand-to-roll-out-digital-diary-app-to-help-people-track-movements-idUSKBN22U0GE; Robbie Harb, “New Zealand releases Bluetooth-free COVID-19 tracing app,” The Register, May 20, 2020, https://www.theregister.com/2020/05/20/new_zealand_scaled_back_digital/.

[19] Jeffrey P. Kahn et al., *Digital Contact Tracing for Pandemic Response, Ethics and Governance Guidance*, 37-38.

[20] There is of course also a need for a layer of cybersecurity so that hostile elements cannot distribute transmitters or receivers that distort the contact data stored by the app, or misuse the data.

[21] Researchers at Oxford believe that the app needs to be installed on at least 80% of all devices, which is approximately 56% of the entire population, in order for it to achieve its purpose — contact tracing — effectively. Their model assumes that people over the age of 70 remained in lockdown, but no traditional contact tracing is underway and no widespread social distancing rules are in place. See: “Digital Contact Tracing Can Slow or Even Stop Coronavirus Transmission and Ease Us Out of Lockdown,” Big Data Institute, April 16, 2020, https://www.bdi.ox.ac.uk/news/digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown; Patrick Howell O’Neill, “No, Coronavirus Apps Don’t Need 60% Adoption to Be Effective,” *MIT Technology Review*, June 5, 2020, https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

[22] Nati Tucker, “The Man Who Controls the Cellphones of a Million Israelis: And What Will Happen If You Dial from a Number that Begins 052-76?” [in Hebrew], The Marker, July 5, 2019, https://www.themarker.com/advertising/.premium-MAGAZINE-1.7449384.

[23] Ankita Chakravarti, “Voluntary Aarogya Setu Now Mandatory in Noida, FIR, Rs 1000 Fine or 6-Mounth Jail if App Not Downloaded,” *India Today*, May 5, 2020, https://www.indiatoday.in/technology/news/story/voluntary-aarogya-setu-now-mandatory-in-noida-fir-rs-1000-fine-or-6-month-jail-if-app-not-downloaded-1674635-2020-05-05; “Coronavirus Lockdown: No More Voluntary, Aarogya Setu App Now Mandatory For Office Workers,” *India Today*, May 1, 2020, https://www.indiatoday.in/technology/news/story/coronavirus-lockdown-no-more-voluntary-aarogya-setu-app-now-mandatory-for-office-workers-1673438-2020-05-01; “Govt of India’s Voluntary Aarogya Setu App Made Mandatory For Smartphone Users In Noida, Greater Noida,” *The Financial Express*, May 5, 2020, https://www.financialexpress.com/industry/technology/govt-of-indias-voluntary-aarogya-setu-app-made-mandatory-for-smartphone-users-in-noida-greater-noida/.

[24] Marc Daalder, “NZ Considering $100m Contact Tracing ‘COVIDCard’,” Newsroom, April 17, 2020, https://www.newsroom.co.nz/2020/04/17/1132682/nz-considering-100m-contact-tracing-covidcard.

[25] See, e.g., Ashkan Soltani, Ryan Calo and Carl Bergstrom, “Contact-tracing Apps are not a Solution to the COVID-19 Crisis,” The Brookings Institution, April 27, 2020, https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/; Marlon Domingus, “Some Troubling Misconceptions About ‘Corona App’,” LinkedIn, April 11, 2020, https://www.linkedin.com/pulse/some-troubling-misconceptions-corona-apps-marlon-domingus/; Marlon Domingus, “Corona Apps, Toilet Paper and Dataism,” LinkedIn, April 18, 2020, https://www.linkedin.com/pulse/corona-apps-toilet-paper-dataism-marlon-domingus/; Jeffrey P. Kahn et al., *Digital Contact Tracing for Pandemic Response, Ethics and Governance Guidance*.

[26] Fred Vogelstein and Will Knight, “Health Officials Say ‘No Thanks’ to Contact-Tracing-Tech.”

[27] Danny Palmer, “Security Experts Warn: Don’t Let Contact-Tracing App Lead to Surveillance,” ZDNet, May 7, 2020, https://www.zdnet.com/article/security-experts-warn-dont-let-contact-tracing-app-lead-to-surveillance/; Darren Dodd, “Contact-Tracing App Raise Surveillance Fears,” *Financial Times*, April 20, 2020, https://www.ft.com/content/005ab1a8-1691-4e7b-8e10-0d3d2614a276.

[28] Amos Toh and Deborah Brown, “How Digital Contact Tracing for COVID-19 Could Worsen Inequality,” Human Rights Watch, June 4, 2020, https://www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality#; Rafael A. Calvo, Sebastian Deterding and Richard M. Ryan, “Health Surveillance During Covid-19 Pandemic,” *BMJ* 369, (April 6, 2020), https://www.bmj.com/content/369/bmj.m1373; Ramesh Raskar et al, “Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic,” PrivateKit: MIT, March 19, 2020, https://arxiv.org/pdf/2003.08567.pdf.

[29] Stuart A. Thompson and Charlie Warzel, “Twelve Million Phones, One Dataset, Zero Privacy,” *The New York Times*, December 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller and Aaron Krolik, “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret,” *The New York Times*, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[30] The right to health is one of a set of internationally agreed human rights standards that have been enumerated in international agreements, including the Universal Declaration of Human Rights, the International Covenant on Economic, Social and Cultural Rights, and the Convention on the Rights of Persons with Disabilities.

[31] Tehilla Shwartz Altshuler and Rachel Aridor Hershkovitz, “Tracking Citizens: What is Going On in the World?”

[32] 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, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html; Min Joo Kim and Simon Denyer, A ‘Travel Log’ of the Times in South Korea: Mapping the Movements of Coronavirus Carriers,” *The Washington Post*, March 13, 2020, https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html.

[33] Thus, according to the guidelines adopted in April 2020. See: “Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak,” European Data Protection Board, adopted April 21, 2020, https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en.

[34] Italy ranks 89th on the Freedom House Global Freedom Scale. See “Global Freedom Scores,” Freedom House, https://freedomhouse.org/countries/freedom-world/scores.

[35] Lorenzo Tondo, “Italy Charges More than 40,000 People with Violating Lockdown,” *The Guardian*, March 18, 2020, https://www.theguardian.com/world/2020/mar/18/italy-charges-more-than-40000-people-violating-lockdown-coronavirus; Eric J. Lyman, “Life Under Coronavirus Lockdown in Italy: My Quarantine, A Worried Wait for a Test Result – and Relief,” *USA Today*, March 12, 2020 https://www.usatoday.com/story/news/health/2020/03/12/coronavirus-milan-rome-italy-quarantine-and-lockdown/5036182002/; Steve Almasy, “An American Woman in Italy has Advice for Life under Countrywide Quarantine: Follow the Rules,” CNN, March 14, 2020, https://www.cnn.com/2020/03/13/europe/italy-american-woman-life-under-quarantine/index.html.

[36] “Italy Says App Tracing Contacts of People Infected With COVID-19 Will Be Anonymous,” *Time*, April 29, 2020, https://time.com/5829665/italy-covid19-app-contact-tracing/; Miles Johnson, Leila Abboud, Helen Warrell, and Tim Bradshaw, “Europe Split Over Approach to Virus Contact Tracing Apps,” *Financial Times*, May 1, 2020, https://www.ft.com/content/10f87eb3-87f9-46ea-88ab-8706adefe72d.

[37] Ranked 94th on the Freedom House Global Freedom Scale.

[38] “Protection against Infection Act,” Government of Germany, July 20, 2000, §§16(4), 17(7), and 19, https://translate.googleusercontent.com/translate_c?depth=1&hl=en&prev=search&pto=aue&rurl=translate.google.com&sl=de&sp=nmt4&u=http://www.gesetze-im-internet.de/ifsg/index.html&usg=ALkJrhhgz_oyvqbzrdBLfA04EgT9RvdW7A.

[39] Christiane Schulzki Haddouti, “Datenschutz: Mit Standortdaten gegen Coronavirus ‘mehr als problematisch,’” [Data Protection: With Location Data Against Coronavirus “More Than Problematic], Heise Online, March 6, 2020, https://www.heise.de/newsticker/meldung/Datenschutz-Mit-Standortdaten-gegen-Coronavirus-mehr-als-problematisch-4677679.html.

[40] Douglas Busvine and Andreas Rinke, “Germany Flips to Apple-Google Approach On Smartphone Contact Tracing,” Reuters, April 26, 2020, https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J.

[41] Ranked 96th on the Freedom House Global Freedom Scale.

[42] Ranked 94th on the Freedom House Global Freedom Scale.

[43] Ranked 93rd on the Freedom House Global Freedom Scale.

[44] Miles Johnson, Leila Abboud, Helen Warrell and Tim Bradshaw, “Europe Split Over Approach to Virus Contact Tracing Apps”; “Next Phase of NHS Coronavirus (COVID-19) App Announced,” U.K. Department of Health and Social Care, June 18, 2020, https://www.gov.uk/government/news/next-phase-of-nhs-coronavirus-covid-19-app-announced.

[45] Ranked 90th on the Freedom House Global Freedom Scale.

[46] The app used in France is StopCovid. See Isobel Asher Hamilton, “France Attacked Apple for not Helping to Build Its Contact-Tracing App,” Business Insider, May 6, 2020, https://www.businessinsider.com/france-attacks-apple-contact-tracing-app-2020-5. The French government criticized Apple’s refusal to refuse to permit the use of the app on its operating system because of its centralized architecture (id.). In the United Kingdom, the app was developed by the digital department of the National Health Service (NHS). According to news reports, though, it is possible that the NHS will change its stance and modify the app to use the decentralized approach, in order to make its use easier and its verification for numbers only of persons in Britain. See: Alex Hern and Kate Proctor, “UK May Ditch NHS Contact-Tracing App for Apple and Google Model,” *The Guardian*, May 7, 2020, https://www.theguardian.com/technology/2020/may/07/uk-may-ditch-nhs-contact-tracing-app-for-apple-and-google-model.

[47] Ranked 97th on the Freedom House Global Freedom Scale.

[48] Kaeli Conforti, "Jacinda Ardern Says, 'Thank You, New Zealand,' as Country Crushes COVID-19," *Forbes*, June 8, 2020, https://www.forbes.com/sites/kaeliconforti/2020/06/08/jacinda-ardern-says-thank-you-new-zealand-as-country-achieves-alert-level-1/#13d4aaf65beb; Amy Gunia, "Why New Zealand's Coronavirus Elimination Strategy Is Unlikely to Work in Most Other Places," *Time*, April 28, 2020, https://time.com/5824042/new-zealand-coronavirus-elimination/; "NZ COVID Tracer App," New Zealand Ministry of Health, https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-resources-and-tools/nz-covid-tracer-app.

[49] Ranked 97th on the Freedom House Global Freedom Scale.

[50] Josh Taylor, "Australia's Covidsafe Coronavirus Tracing App Works as Few as One In Four Times for Some Devices," *The Guardian*, June 17, 2020, https://www.theguardian.com/australia-news/2020/jun/17/covid-safe-app-australia-covidsafe-contact-tracing-australian-government-covid19-tracking-problems-working.

[51] Ranked 86th on the Freedom House Global Freedom Scale.

[52] Fred Vogelstein & Will Knight, "Health Officials Say 'No Thanks' to Contact-Tracing Tech"; Jack Kelly, "Contact Tracing: A Newly Created 'Big Brother' Bureaucracy Tracks Down COVID-19 – Infected People and Those Who Have Been in Contact with Them."

[53] Mike Peterson, "Utah Declines Apple-Google Exposure Notification API for App Made by Social Media Start-up," AppleInsider, May 14, 2020, https://appleinsider.com/articles/20/05/13/utah-declines-apple-google-exposure-notification-api-for-app-made-by-social-media-startup; Aaron Holmes and Hugh Langley, "Apple and Google's ambitious COVID-19 contact-tracing tech can help contain the pandemic if used widely. But so far only 3 states have agreed – and none has started to use it," Business Insider, June 10, 2020, https://www.businessinsider.com/apple-google-coronavirus-contact-tracing-tech-states-dont-plan-using-2020-6.

[54] Ranked 93rd on the Freedom House Global Freedom Scale.

[55] "Communication Disease Control Act," Government of Taiwan, January 20, 2004, §11, 26, 31, and 39, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=L0050001.

[56] Kathrin Hille and Edward Whife, "Containing Coronavirus: Lessons From Asia," *Financial Times*, March 16, 2020, https://www.ft.com/content/e015e096-6532-11ea-a6cd-df28cc3c6a68; C. Jason Wang, Chun Y. Ng, and Robert H. Brook, "Response to COVID-19 in Taiwan: Big Data Analytics, New Technology, and Proactive Testing," *JAMA* 323, no. 14 (March 3, 2020): 1341-1342, https://jamanetwork.com/journals/jama/fullarticle/2762689.

[57] Benjamin Powers, "Mass Surveillance Threatens Personal Privacy Amid Coronavirus," CoinDesk, March 12, 2020, https://www.coindesk.com/mass-surveillance-threatens-personal-privacy-amid-coronavirus; Michelle Yun, "How Taiwan is Containing Coronavirus – Despite Diplomatic Isolation by China," *The Guardian*, March 13, 2020, https://www.theguardian.com/world/2020/mar/13/how-taiwan-is-containing-coronavirus-despite-diplomatic-isolation-by-china.

[58] Kathrin Hille & Edward Whife, "Containing Coronavirus: Lessons From Asia"; Josh Rogin, "The pandemic shows why Taiwan is a far better partner than the People's Republic," *The Washington Post*, May 8, 2020, https://www.washingtonpost.com/opinions/global-opinions/the-pandemic-shows-why-taiwan-is-a-far-better-partner-than-the-peoples-republic/2020/05/07/8af1e1c8-909d-11ea-a9c0-73b93422d691_story.html; Andrew Leonard, "Taiwan is beating the Coronavirus. Can the US do the same?," *Wired*, March 18, 2020, https://www.wired.com/story/taiwan-is-beating-the-coronavirus-can-the-us-do-the-same/.

[59] Nicola Smith, "Taiwan Offers Its Contact Tracing Apps to UK," *The Telegraph*, May 9, 2020, https://

www.telegraph.co.uk/news/2020/05/09/taiwan-offers-contact-tracing-apps-uk/.

[60] Ranked 83rd on the Freedom House Global Freedom Scale.

[61] "Infectious Disease Control and Prevention Act," Government of South Korea, December 29, 2009, §81(5), (8), https://elaw.klri.re.kr/eng_mobile/ganadaDetail.do?hseq=37239&type=abc&key=INFECTIOUS%20DISEASE%20CONTROL%20AND%20PREVENTION%20ACT&param=I.

[62] Ibid., §§38 and 74.

[63] Justin Fendos, "How Surveillance technology powered South Korea's COVID-19 response," The Brookings Institution, April 29, 2020, https://www.brookings.edu/techstream/how-surveillance-technology-powered-south-koreas-covid-19-response/.

[64] Rory Cellan-Jones, "Tech Tent: Can We Learn About Coronavirus – Tracing From South Korea?" BBC, May 15, 2020, https://www.bbc.com/news/technology-52681464; Aaron Holmes, "South Korea is Relying on Technology to Contain COVID-19, Including Measures that Would Break Privacy Laws in the US – and So Far, It's Working," Business Insider, May 2, 2020, https://www.businessinsider.com/coronavirus-south-korea-tech-contact-tracing-testing-fight-covid-19-2020-5.

[65] The Privacy Protection Law 5741-1981 is out of date and not adequate for the digital age, even though it has been amended several times and even though the Privacy Protection Regulations (Data Security) 5777-2017 enacted pursuant to the law, which came into effect in May 2018, include a number of advanced provisions related to the protection of data and privacy. The European Union recognized the adequacy of the Israeli regulations to the European privacy protection standard in 2011. See "Commission Decision of 31 January 2011 Pursuant to Directive 95/46/EC of European Parliament and of the Council on the Adequate Protection of Personal Data of the State of Israel with regard to Automated Processing of Personal Data," Notified under document C(2011) 332) (2011/61/EU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061. But after the introduction of the GDPR in May 2018, the EU began reexamining the adequacy decisions issued in the past. Israel's deficient and outdated privacy protection legislation raises serious doubts that the EU will be willing to issue a new decision that Israeli law is adequate to the current European rules. The authorization of the GSS to conduct involuntary digital contact tracing of Israeli citizens during the current emergency further increases the fear that the European Commission will refuse to recognize the adequacy of Israeli law. See Christopher Docksey & Christopher Kuner, "The Coronavirus Crisis and EU Adequacy Decisions for Data Transfer," European Law Blog, April 3, 2020, https://europeanlawblog.eu/2020/04/03/the-coronavirus-crisis-and-eu-adequacy-decisions-for-data-transfers/.

[66] According to data published by the OECD in November 2019, Israel invested significantly less in its healthcare system than most of the OECD members. Only 15 countries rank below Israel on this index, including India, Turkey, and Morocco. The annual per capita outlay on healthcare in Israel is $2,780; the OECD average for medical services is $4,000. In Israel, the annual budget for the healthcare system is only 5.7% of GDP; the OECD average is 8.8%. See "Health at a Glance 2019," (OECD, November 7, 2019), http://www.oecd.org/health/health-systems/health-at-a-glance-19991312.htm.

[67] This category refers to two entities: the National Emergency Authority and the IDF Homefront Command. There was also a strong response by other defense and security agencies, including the Mossad, the GSS, and elite and intelligence units of the IDF. In addition, the National Security Council (which is part of the Prime Minister's Office), which was made responsible for coordinating the response to the pandemic, is staffed mainly by former defense establishment personnel.

[68] "Public Health Ordinance," Government of Israel, 1940, https://www.health.gov.il/LegislationLibrary/

Sherutei03.pdf.

[69] “Public Health Order (the Novel Coronavirus) (Home Isolation and Miscellaneous Provisions) (ad hoc provisions) 5780-2020 (hereinafter: Home Isolation Order),” Government of Israel, February 20, 2020, https://www.nevo.co.il/law_html/law01/502_230.htm. The order has since been modified and the quarantine provisions extended to match the spread of the coronavirus in Israel and the world.

[70] The Basic Law: The Knesset.

[71] According to a study conducted by Nir Kosti, a graduate student at the Hebrew University, and Yoav Mehozai of the School of Criminology at the University of Haifa, no fewer than 70 emergency regulations have been enacted since the start of the coronavirus crisis — more than in any year since independence, including wartime. See Shahar Ilan, “The Government Has Broken the Record for Emergency Regulations” [in Hebrew], Calcalist, April 27, 2020, https://www.calcalist.co.il/local/articles/0,7340,L-3811853,00.html.

[72] The General Security Service Law 5662-2002, Israeli Knesset.

[73] Ronen Bergman and Ido Schwarztuch, “‘The Tool’ is Exposed: The GSS’s Secret Database that Collects Your Text Messages, Calls, and Location” [in Hebrew], *Yedioth Ahranoth*, March 27, 2020, https://www.yediot.co.il/articles/0,7340,L-5701611,00.html.

[74] The first attempt was the passage of the Emergency Regulations (Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus) 5780-2020, Israeli Knesset. This was repealed by Government Resolution 4950 of March 31, 2020: “Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus and repeal of the Government resolution.” Subsequently this decision, too, was revoked, and replaced by Government Resolution 4916, March 24, 2020 (“Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus”), which was approved by the Knesset Foreign Affairs and Defense Committee.

[75] See Amir Cahane, “The Israeli Emergency Regulations for Location Tracking of Coronavirus Carriers,” Lawfare, March 31, 2020, https://www.lawfareblog.com/israeli-emergency-regulations-location-tracking-coronavirus-carriers; Amir Cahane and Yuval Shany, “Regulation of Online Surveillance in Israeli Law and Comparative Law” [in Hebrew], (Israel Democracy Institute, 2019), https://www.idi.org.il/media/13074/regulation.pdf.

[76] Government Resolution 4916, “Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus,” March 24, 2020, https://www.gov.il/he/departments/policies/dec4916_2020.

[77] HCJ 2109/20, *Adv. Shahar Ben Maher et alii v. the Prime Minister et al.*; HCJ 2135/20, *the Association for Civil Rights in Israel v. the Prime Minister et al.*; HCJ 2141/20, *Adalah, the Legal Center for Arab Minority Rights in Israel et al. v. the Prime Minister et al*, [in Hebrew], April 26, 2020, https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts%5C20%5C090%5C021%5Cv43&fileName=20021090.V43&type=2.

[78] HCJ 2109/20, *Adv. Shahar Ben Maher et al. v. the Prime Minister et al.*, [in Hebrew], March 19, 2020, https://supremedecisions.court.gov.il/Home/Download?path=HebrewVerdicts%5C20%5C090%5C021%5Cv09&fileName=20021090.V09&type=2.

[79] Government Resolution 4950, “Empowerment of the General Security Service to assist the national

effort to reduce the spread of the novel coronavirus and repeal of the Government resolution," [in Hebrew] March 31, 2020, https://www.gov.il/he/departments/policies/dec4950_2020. Subsequently this decision, too, was revoked, and replaced by Government Resolution 4916, "Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus," [in Hebrew] March 24, 2020, https://www.gov.il/he/departments/policies/dec4916_2020.

80 Government Resolution 5042, "Extension of the Validity of the Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus, and promotion of the legislative process," May 4, 2020, https://www.gov.il/he/departments/policies/dec5042_2020.

81 "Press release: The Intelligence Services Subcommittee granted the Government an extension of only three weeks for continuing to use the GSS tool in the battle against Corona, in order to permit the legislative process to proceed," The Knesset Foreign Affairs and Defense Committee News, May 5, 2020, https://main.knesset.gov.il/Activity/committees/ForeignAffairs/News/Pages/pr_050520.aspx.

82 Zvi Zerahiah, "Coronavirus Cabinet Rules: The GSS will stop its cellular location of citizens" [in Hebrew], Calcalist, June 8, 2020, https://www.calcalist.co.il/local/articles/0,7340,L-3831671,00.html.

83 Oded Yaron, "Users Report Mistakes in Identification of Proximity to Coronavirus Patients by the Hamagen App" [in Hebrew], *Ha'aretz*, March 28, 2020, https://www.haaretz.co.il/captain/software/.premium-1.8719020; Raphael Kahan, "The Health Crisis: A Bug in the Hamagen App that Identifies Coronavirus Patients" [in Hebrew], Calcalist, March 29, 2020, https://www.calcalist.co.il/internet/articles/0,7340,L-3804591,00.html; Adir Janko, "The Health Ministry on the Bug in the Hamagen App: 'Use your Best Judgment'" [in Hebrew], Ynet, March 29, 2020, https://www.ynet.co.il/articles/0,7340,L-5703517,00.html.

84 At the High Court hearing on April 14, 2020, Shosh Shmueli of the High Court division of the State Prosecutor's Office reported that 1.5 million people had installed the app, of whom 400,000 had subsequently removed it from their devices. See Avishai Greenzweig, "At Globes Request, Today's High Court Hearing was Live-Streamed" [in Hebrew], Globes, April 16, 2020, https://www.globes.co.il/news/article.aspx?did=1001325439.

85 "Authorizing the GSS to assist in the national effort to minimize the spread of the novel COVID-19 virus (temporary order), 5780 – 2020," Government of Israel, July 1, 2020 [in Hebrew].

86 "A bill for regulating technological means for assisting in the national effort to minimize the spread of the novel COVID-19 virus (authorizing the GSS and the development of civil contact tracing technologies), 5780 – 2020," Government of Israel, July 15, 2020 [in Hebrew].

87 For example, in the first week on July 2020 (July 1-July 8) there were 8526 new COVID-19 cases in Israel. See Israel Ministry of Health, "COVID-19 in Israel – General Situation Report," July 18, 2020, https://datadashboard.health.gov.il/COVID-19/?utm_source=go.gov.il&utm_medium=referral. During the same period, only 2,468 new COVID-19 cases were identified solely using the GSS. See The Legal Department, Israel Ministry of Health, "Report according to the Authorizing the GSS to assist in the national effort to minimize the spread of the novel COVID-19 virus (temporary order), 5780 – 2020," Government of Israel, July 1, 2020 [in Hebrew]. Meaning, the GSS assisted in identifying only 34.5% of new COVID-19 cases that week. See also: Omer Kabir, "One Third of the persons with COVID-19 in Israel were allocated using the GSS's surveillance tool" [in Hebrew], Calcalist, May 25, 20, https://www.calcalist.co.il/internet/articles/0,7340,L-3827032,00.html.

88 i24News, "Health Ministry admits more than 12,000 Israelis quarantined by mistake," i24NEWS, July 14, 2020, https://www.i24news.tv/en/news/israel/1594736977-health-ministry-admits-more-than-12-000-israelis-quarantined-by-mistake.

89 “Public Health Ordinance,” Government of Israel.

90 General Data Protection Regulation 2016/679, European Commission, April 14, 2016, implementation date May 25, 2018, https://gdpr-info.eu/.

91 With the exception of Covtracer in Cyprus, Rakning C-19 in Iceland, and ViruSafe in Bulgaria.

92 See references 12-15.

93 Yaron Drukman, “The health ministry data: 3 times more COVID-19 cases a day comparing to the first wave,” Ynet, July 5, 2020, https://www.ynet.co.il/articles/0,7340,L-5759488,00.html.

94 Government Resolution 5042, “Extension of the Validity of the Empowerment of the General Security Service to assist the national effort to reduce the spread of the novel coronavirus, and promotion of the legislative process.”

95 Zvi Zerahiah, “Coronavirus Cabinet Rules: The GSS will stop its cellular location of citizens” [in Hebrew], Calcalist, June 8, 2020, https://www.calcalist.co.il/local/articles/0,7340,L-3831671,00.html.

96 “Authorizing the GSS to assist in the national effort to minimize the spread of the novel COVID-19 virus (temporary order), 5780 – 2020,” Government of Israel, July 1, 2020 [in Hebrew].

97 “A bill for regulating technological mean for assisting in the national effort to minimize the spread of the novel COVID-19 virus (Authorizing the GSS and the development of civil contact tracing technologies), 5780 – 2020,” Government of Israel, July 15, 2020 [in Hebrew].

98 Christopher Docksey and Christopher Kuner, “The Coronavirus Crisis and EU Adequacy Decisions for Data Transfer.”

99 Benjamin Netanyahu, “Israel Achievements in the fight against COVID-19 serve as a model for many countries,” (speech, Israel, May 4, 2020).

100 Itamar Eichner, “Netanyahu: ‘On June 14 We Will Abolish the Restrictions on Public Assembly; the Preschools will return on Sunday’” [in Hebrew], Ynet, May 4, 2020, https://www.ynet.co.il/articles/0,7340,L-5725006,00.html.

101 Kaeli Conforti, “Jacinda Ardern Says, ‘Thank You, New Zealand,’ as Country Crushes COVID-19”; Amy Gunia, “Why New Zealand’s Coronavirus Elimination Strategy Is Unlikely to Work in Most Other Places”; “NZ COVID Tracer App,” New Zealand Ministry of Health.

102 For more on this topic, see: Yagil Levy, *Who Rules the Armed Forces? Between Supervision of the Armed Forces and Military Rule* [in Hebrew], (Magnes Press, 2010); Asaf David, “Military-Civilian Relations in Israel: The Debate and the Missing Link” [in Hebrew], *Theory and Criticism* 41 (2013), https://theory-and-criticism.vanleer.org.il/wp-content/uploads/woocommerce_uploads/2016/12/Teoria-41_David.pdf.

103 Chen Ma’anit, “The ‘Securitization’ of the Coronavirus Crisis is a Dangerous Precedent. The Military Shouldn’t be Managing It” [in Hebrew], Globes, April 7, 2020, https://www.globes.co.il/news/article.aspx?did=1001324729; Stewart Cohen and Meir Elran, “Patterns of Military Action in the War against the Coronavirus: Lessons for Israel from the Experience of Others, Overview” (Institute for National Security Studies, April 2020), https://www.inss.org.il/publication/the-army-and-the-fight-against-the-coronavirus/.

104 Tamar Hermann, Or Anabi, William Cubbison, and Ella Heller, “Israeli Democracy Index 2019,” (Israel Democracy Institute, January 2020), https://en.idi.org.il/publications/29559.

105 Tamar Hermann and Or Anabi, “Israeli Voice Index: In the Shadow of the Coronavirus Crisis, 76% of Israelis are Afraid of Catching the Virus,” (Israel Democracy Institute, March 30, 2020), https://en.idi.org.il/articles/31155.

106 See reference 67.

107 In reaction to the coronavirus pandemic, the justice minister declared a state of emergency in the court system. As a result, the start of the prime minister’s trial was delayed from March 17, 2020, to May 24. See Daniel Dolev and Tal Shalev, “After the Freezing the Courts’ Operation: Opening of Netanyahu’s Trial Postponed for Two Months” [in Hebrew], WallaNews, March 15, 2020, https://news.walla.co.il/item/3346575.

108 The Temporary Subcommittee for Intelligence Matters and the Secret Services held five sessions on approving the government resolution, as required by §7(b)(6) of the General Security Service Law: “Press release: At the end of marathon deliberations and after adding restrictive amendments, the Knesset Temporary Subcommittee on GSS Affairs ratified the Government resolution empowering the GSS to assist the battle to limit the spread of the coronavirus,” The Knesset Foreign Affairs and Defense Committee News, March 31, 2020, https://main.knesset.gov.il/Activity/committees/ForeignAffairs/News/Pages/pr_310320.aspx.

109 See reference 77.

110 Asaf Malhi, Gilad Malach, and Shuki Friedman, “How is the Ultra-Orthodox Sector Coping with the Coronavirus” [in Hebrew], (Israel Democracy Institute, March 26, 2020), https://www.idi.org.il/articles/31128; Aaron Rabinowitz, “Their Detachment from Israeli Society Makes it Difficult for the Ultra-Orthodox to Check the Spread of the Coronavirus” [in Hebrew], *Ha’aretz*, April 2, 2020, https://www.haaretz.co.il/health/corona/.premium-1.8732613.

111 Gideon Lewis-Kraus, “How to Make Government Trustworthy Again,” *Wired*, June 18, 2020, https://www.wired.com/story/how-to-make-government-trustworthy-again/.

112 Danny Zaken, Tal Schneider, and Anat Bein-Lubovitch, “Israel Democracy Institute: The Israeli Public has Confidence in the Armed Forces and the President—but Much Less in Everything Else” [in Hebrew], Globes, January 7, 2020, https://www.globes.co.il/news/article.aspx?did=1001313885.

113 Shira Kadari-Ovadia, Noa Spiegel, and Bar Peleg, “With a Health Declaration and Face Mask: First- to Third-Graders Returned to School from their Coronavirus Vacation” [in Hebrew], *Ha’aretz*, May 3, 2020, https://www.haaretz.co.il/health/corona/.premium-MAGAZINE-1.8816661.

114 “Authorizing the GSS to assist in the national effort to minimize the spread of the novel COVID-19 virus (temporary order), 5780 – 2020,” Government of Israel, July 1, 2020 [in Hebrew].

115 The Legal Department, Israel Ministry of Health, “Report according to the Authorizing the GSS to assist in the national effort to minimize the spread of the novel COVID-19 virus (temporary order), 5780 – 2020,” Government of Israel, July 1, 2020 [in Hebrew].

116 State of Israel, Ministry of Health, Mobile Phone Tracking Text Messages, https://govextra.gov.il/ministry-of-health/corona/corona-virus-en/.

117 Toi Staff, “Phone tracking sends thousands to isolation, but many says system makes mistakes,” *The Times of Israel*, July 6, 2020, https://www.timesofisrael.com/phone-tracking-sends-thousands-to-isolation-but-many-say-system-makes-mistakes/; Danny Zaken, “The GSS’s locations missed in about 5% since last Thursday,” Globes, July 5, 2020 [in Hebrew], https://www.globes.co.il/news/article.aspx?did=1001334706; Adir Yanko, “GSS Locations are Back, the Hotline Collapsed: “Hours online, and Appealing is Impossible,” Ynet, July 4, 2020 [in Hebrew], https://www.ynet.co.il/articles/0,7340,L-5759140,00.html.

118 i24News, “Israelis to sue state over ’wrongful’ virus quarantine orders,” Ynet, July 8, 2020, https://www.ynetnews.com/article/rkN9OI7JP.

119 Tamar Hermann and Or Anabi, “Israeli Voice Index: Israel in Times of Corona,” The Israel Democracy Institute, July 14, 2020, https://en.idi.org.il/articles/32010.

120 Ibid.

121 Michele J. Gelfand et al, “Differences Between Tight and Loose Cultures: A 33-Nation Study,” *Science* 332, no. 6033 (2011): 1100-1104, https://digitalcommons.ilr.cornell.edu/cgi/viewcontent.cgi?article=2302&context=articles.

122 Jason Horowitz and Emma Bubola, “On Day 1 of Lockdown, Italian Officials Urge Citizens to Abide by Rules,” *The New York Times*, March 8, 2020, https://www.nytimes.com/2020/03/08/world/europe/italy-coronavirus-quarantine.html.

123 See references 12-15.

124 See reference 84. In Singapore, as of May 1, 2020, only 20% of the population, or 1.1 people, had downloaded the TraceTogether app, launched at March 20, 2020. See Yip Wai Yee, “Coronavirus: More Need to Use Contact Tracing App for it to be Effective,” *The Straits Times*, May 1, 2020, https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effective.

125 In Australia, the federal government put a lot of efforts in encouraging the public to install the app including explaining the importance of its installation by as many people as possible, running an extensive media campaign that included video clips, billboard advertisements, radio reports, and posts on social networks. The prime minister gave multiple media interviews and explained that installation of the app was the key for a gradual return to routines and restarting the economy. He also compared the app to sunscreen: The app, he said, would protect users and their families, healthcare personnel, and, ultimately, the livelihoods of users and their families, because it would permit the reopening of the Australian economy. The media efforts bore fruit: Within 10 days, the app was installed by a record number of 5 million users. See “COVIDSafe App Campaign Resources,” Australian Government Department of Health, https://www.health.gov.au/resources/collections/covidsafe-app-campaign-resources; “Australians Urged to Sign Up to Tracking App,” BBC News, April 29, 2020, https://www.bbc.com/news/world-australia-52476262; “Treat Tracing App Like Sunscreen: Aussie PM,” *Otago Daily Times*, April 29, 2020, https://www.odt.co.nz/news/australia/treat-tracing-app-sunscreen-aussie-pm; “Coronavirus Tracing App CovidSafe Hits 5 Million Downloads as Government Concedes Incompatibility With Older Phones,” ABC News, May 6, 2020, https://www.abc.net.au/news/2020-05-06/coronavirus-covidsafe-5-million-download-officials-concede-flaws/12221004.

126 Michelle M. Mello and C. Jason Wang, “Ethics and Governance for Digital Disease Surveillance,” *Science* 368, no. 6494 (May 11, 2020): 951-954, https://science.sciencemag.org/content/sci/368/6494/951.full.pdf.

127 Marc Daalder, “NZ Considering $100m Contact Tracing ‘COVIDCard’.”

128 “The DP-3T Project, Security and Privacy Analysis of the Document ‘PEPP-PT: Data Protection and Information Security Architecture’,” April 19, 2020, https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf.

129 David M. Halbfinger, “Israeli Army’s Idea Lab Aims at a New Target: Saving Lives,” *The New York Times*, May 7, 2020, https://www.nytimes.com/2020/05/07/world/middleeast/coronavirus-israel.html; Tal Shahaf, “The Start-Up Nation Enlists in the Battle against the Coronavirus” [in Hebrew], Ynet, March 26, 2020, https://www.ynet.co.il/articles/0,7340,L-5701569,00.html; Sagi Cohen, “Electronic Nose and Digital Certificate: How Technology will Keep Us Healthy after Corona” [in Hebrew], The Marker, April 9, 2020, https://www.themarker.com/coronavirus/.premium-MAGAZINE-1.8747778.

ABOUT THE AUTHORS

Tehilla Shwartz Altshuler is a senior fellow at the Israel Democracy Institute and head of the institute's Democracy in the Information Age Program. Her research and public activity focus on technology and media law, policy, and ethics. She holds a LL.D. from the Hebrew University of Jerusalem, and completed her post-doctoral studies at the Kennedy School of Government at Harvard University.

Rachel Aridor Hershkovitz is a researcher at the Israel Democracy Institute. She has an LL.M. degree in trade regulation, focusing on intellectual property, from New York University School of Law and is currently a Ph.D. candidate at Haifa University's Faculty of Law.

ACKNOWLEDGMENTS

Anna Newby edited this paper, with assistance from Morgan Smith, and Rachel Slattery provided layout.

Brookings recognizes that the value it provides is in its absolute commitment to quality, independence, and impact. Activities supported by its partners reflect this commitment. The conclusions and recommendations of any Brookings research are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars.

BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
brookings.edu