Assessing the Governance of Digital Contact Tracing in Response to COVID-19: Results of a Multi-National Study

Brian Hutler,[1] *Alessandro Blasimme,*[2] *Rachel Gur-Arie,*[3] *Joseph Ali,*[4] *Anne Barnhill,*[4] *Amelia Hood,*[4] *Jeffrey Kahn,*[4] *Nancy L. Perkins,*[5] *Alan Regenberg,*[4] *and Effy Vayena*[2]

1. TEMPLE UNIVERSITY, PHILADELPHIA, PA, USA; 2. ETH ZÜRICH, ZURICH, SWITZERLAND; 3. ARIZONA STATE UNIVERSITY, PHOENIX, AZ, USA; 4. JOHNS HOPKINS UNIVERSITY, BALTIMORE, MD, USA; 5. ARNOLD & PORTER KAYE SCHOLER LLP, WASHINGTON, DC, USA.

Keywords: Digital Contact Tracing, Pandemic Response, Public Health Governance, Public Health Ethics

Abstract: This paper describes the results of a multi-country survey of governance approaches for the use of digital contact tracing (DCT) in response to the COVID-19 pandemic. We argue that the countries in our survey represent two distinct models of DCT governance, both of which are flawed. The "data protection model" emphasizes privacy protections at the expense of public health benefit, while the "emergency response model" sacrifices transparency and accountability, prompting concerns about excessive governance surveillance. The ethical and effective use of DCT in the future requires a new governance approach that is better suited to this novel use of mobile phone data to promote public health."

Introduction

In response to the COVID-19 pandemic, many countries developed and deployed digital contact tracing (DCT) systems utilizing data collected from users' mobile phones. This paper describes the laws and policy instruments employed by nine countries to authorize and regulate the use of DCT technology. Our analysis provides an overview of the governance approaches adopted by countries in the design and implementation of DCT technology. We found that the countries surveyed employed one of two distinct governance approaches: a Data Protection Model, focused primarily on legislative instruments aimed at creating a legal basis for DCT systems in the context of rigorous data protection and privacy safeguards; or an Emergency Response Model, focused on expanding executive prerogatives with the aim of gathering as much data as efficiently as possible to help prevent the spread of COVID-19. Analyzing the strengths and weaknesses of these contrasting DCT governance models should contribute to developing more nuanced governance approaches for the future use of DCT, as well as other digital public health technologies.

Our analysis suggests that neither the Data Protection Model nor the Emergency Response Model was

Brian Hutler, J.D., Ph.D., *is Assistant Professor of Philosophy at Temple University.* **Alessandro Blasimme, Ph.D.**, *is Professor of Bioethics at ETH Zürich.* **Rachel Gur-Arie, Ph.D.**, *is Assistant Professor in Health Services Research at the Edson College of Nursing and Health Innovation at Arizona State University.* **Joseph Ali, J.D.**, *is Assistant Professor in the Department of International Health at the Johns Hopkins University Bloomberg School of Public Health.* **Anne Barnhill, Ph.D.**, *is Associate Research Professor at the Johns Hopkins University Berman Institute of Bioethics.* **Amelia Hood, M.A.**, *is a Research Associate at the Johns Hopkins University Berman Institute of Bioethics.* **Jeffrey Kahn, M.P.H., Ph.D.**, *is the Andreas C. Dracopolous Director of the Johns Hopkins University Berman Institute of Bioethics.* **Nancy L. Perkins, J.D.**, *serves as Counsel at Arnold & Porter Kaye Scholer LLP (Washington, DC).* **Alan Regenberg, M.B.E.**, *is the Director of Outreach and Research Support, and a core faculty member at the Johns Hopkins University Berman Institute of Bioethics.* **Effy Vayena, Ph.D.**, *is Professor of Bioethics at ETH Zürich.*

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804.
DOI: https://doi.org/10.1017/jme.2023.20

ideally suited to the governance of DCT. Emergency response laws provide few protections against the government's use of citizens' data, prompting concerns about lack of transparency and accountability. Data protection laws, on the other hand, are designed primarily to protect against invasions of users' privacy; yet in a critical pandemic, there may be overriding public health goals that render the privacy objective more of a hindrance than a societal benefit.

contact tracing. Although there were earlier, smaller-scale earlier attempts to use DCT,[4] the COVID-19 pandemic prompted a much more significant effort on the part of many national governments to collect data via mobile phones to augment traditional contact tracing on a large scale.

This paper surveys the governance approach employed by nine countries that utilized mobile phone-based DCT technology in response to COVID-19: Australia, France, Ghana, Israel, Italy, South Africa, South Korea, Switzerland, and the United States. (Each country's approach to DCT governance is summarized in Table 1, below.) Because France and Italy are members of the European Union (EU), we also discuss the EU's approach to DCT governance. We selected these nine countries based on their geographic diversity and the public availability of relevant legal materials accessible to members of the author group. All of these countries, except for the United States, enacted legislation or policy at the national level that was specifically tailored to authorizing and regulating the use of DCT in response to COVID-19. These DCT-specific laws fell into two categories. In Australia, France, Italy, and Switzerland, the government authorized the use of DCT by enacting laws designed to be consistent with existing data protection laws. The remaining four countries — Ghana, Israel, South Korea, and South Africa — authorized the use of DCT under their emergency response laws. We discuss each group in turn.

This paper surveys the governance approach employed by nine countries that utilized mobile phone-based DCT technology in response to COVID-19: Australia, France, Ghana, Israel, Italy, South Africa, South Korea, Switzerland, and the United States.

We argue that a new approach to DCT governance is needed to maximize the benefits of this technology for future infectious disease outbreaks. Current research suggests that DCT employed during COVID-19 helped to reduce transmission when the system was widely adopted;[1] but low uptake tended to undermine effectiveness.[2] Governance of DCT must strike the right balance between mandating use of the technology and fostering trust and voluntary adoption. Governments must implement oversight and accountability mechanisms, prevent the misuse of personal data, provide transparency regarding the functionality of DCT, and deploy an effective communication strategy to explain the public health uses and benefits of the technology. We recommend that, as we move beyond "first generation" DCT, countries that utilize DCT technology in the future develop a tailored governance approach capable of effectively regulating and communicating about this new form of public health intervention.

1. Contrasting Governance Models

Contact tracing is a public health tool that is traditionally employed by public health agencies to identify and alert individuals who have been exposed to an infectious disease agent in order to recommend or impose quarantine or other measures designed to limit further spread of the pathogen.[3] "Digital contact tracing" (DCT) refers to a broad category of technologies used to facilitate the identification of individuals who may have been exposed to an infectious agent such as the virus that causes COVID-19, SARS-CoV-2. DCT is a novel form of technology that holds promise to valuably automate and scale up traditional public health

1.1 The Data Protection Model

The countries discussed in this section adopted a "Data Protection Model" of DCT governance. This model has two distinctive features: First, the countries that adopted this model enacted DCT-specific laws as amendments to or ordinances under existing data protection laws. Second, the model is grounded in the principle of data minimization, which holds that the least possible amount of personally identifiable information necessary to achieve a given purpose should be collected, used, and disclosed.

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

The European Union

The **European Union** (EU) adopted governance of DCT technology by means of guidance issued by the European Commission (EC) on April 17, 2020 (2020/C 124 I/01).[5] The EC guidance identifies privacy and data protection as paramount policy concerns in implementing DTC. In particular, the EC guidance stresses the importance of data minimization and sets very rigid limits for data disclosure, use, and storage, consistent with the EU's regulation governing the protection of personal data, the General Data Protection Regulation (GDPR).[6]

The EC Guidance tends to support a "decentralized" approach to DTC, in which data collected from mobile phone users is stored in their phones and contact tracing is activated from that locally stored data. This is in contrast to a "centralized" approach in which data are transmitted to a central database where contacts between users are identified and from which contacts with infected users are notified to those exposed. The EC left member states leeway to adopt either the centralized or decentralized approach.

During the early weeks of the pandemic, a group of European IT experts had created a consortium, known as Pan-European Privacy - Preserving Proximity Tracing protocol (PEPP-PT), which aimed at developing a centralized DCT protocol. Countries such as Germany, France, and the United Kingdom had already begun the development of their national DCT systems based on such a protocol, when another group of experts (some initially part of PEPP-PT) formed an alternative consortium focused on the creation of a decentralized model: the Decentralized Privacy-Preserving Proximity Tracing, or DP-3T for short. DP-3T also included experts from outside the European Union, including from the Swiss Federal Institutes of Technology of Lausanne (EPFL) and Zurich (ETH). Based on specifications from the DP-3T protocol, Google and Apple created an API for the development of apps on mobile phones running Android and iOS, which is known as the Google Apple Exposure Notification (GAEN) system.

The GAEN system relies on low-energy Bluetooth signals sent between mobile phones to record "proximity events," that is, instances in which a user is in proximity to another user, usually defined as within six feet or two meters for a specified period of time (e.g., 15 minutes). When a proximity event occurs, the users' phones exchange encrypted "tokens," each of which corresponds to the other user's cell phone but is anonymous as to the other user's identity. These tokens are stored on the users' phones for a specified period of time (e.g. 14 days). Users are instructed to report into the GAEN app on their phone if they test positive for SARS-CoV-2. If a user reports a positive test, all other users who have the infected user's token stored on their phone receive push notifications warning them of their potential exposure, but without revealing any information about the time of the exposure or the identity of the contact.[7] The GAEN system is "decentralized" because the record of these proximity events is stored exclusively on the various users' phones, not in a government or corporate database.

Italy

The availability of GAEN induced some European countries, including **Italy**, to adopt a decentralized approach to DCT. In June 2020, Italy released an app called Immuni based on the GAEN system. The legal basis for the Immuni app was an executive decree, issued by the Government on April 30, 2020 to specify the legal framework for the use of a national contact-tracing app and to address particular issues regarding accountability and data protection and privacy, in compliance with the GDPR.[8] The decree provides that: (1) the technical platform of the Italian DCT system should be entirely located on the national territory, (2) clear and exhaustive information should be provided to users before the activation of the app, (3) only essential data may be collected, which may not include user geolocation data, (4) the collected data may be used only for specified purposes and should be regularly erased, and (5) the system should be deactivated by the end of 2020. On June 1, 2020, following a privacy impact assessment by the Ministry of Health, the national commission for the protection of personal data (the "Garante per la Protezione dei Dati Personali" or GPDP) gave a green light to use of the decentralized Immuni app,[9] and two weeks later, the app was made available to the whole population.

France

The **French** government — following the advice of a dozen public expert bodies[10] — opted for a centralized approach to collecting proximity data that did not rely on the GAEN system. On May 29, 2020, the French government issued an ad hoc decree to clarify the legal bases for the French DCT system[11] and on June 2, 2020, made available an app called StopCovid.[12] The decree specified the type of data being collected, the time-limits for data collection (limited to 6 months after the end of the emergency period) and how relevant principles of the GDPR were taken into account in the app's design.

The French Government's rationale for the centralized system was twofold. First, the government argued

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

that the involvement of big tech companies with the decentralized approach (GAEN) is inappropriate as it undermines the prerogatives of the state in matters of public health protection. Second, the government argued that the centralized approach is more privacy-preserving because, rather than transmitting proximity data from one user's phone to another's, the StopCovid app sends each user's data to the central server, whereas in the decentralized approach, this information was sent to all users' smartphones.[13]

Switzerland

In other countries, policymakers amended existing data protection laws to create specific requirements regarding DCT in the context of the COVID-19 pandemic. **Switzerland** introduced new articles to its Epidemics Act of 2012 (818.101) to define the legal framework for DCT systems. Under Article 60 of the Epidemics Act, the Swiss Federal Office of Public Health already had authority over the collection and use of personal data — including contact information — for public health purposes. A federal law of June 19, 2020 (AS 2020 2191) introduced a provisional specific article (60a) to create a legal basis for the implementation of DCT in the country. The legislation stresses that individuals may voluntarily choose whether to use the national DCT app and prohibits enterprises and other private actors from either benefitting from or penalizing anyone for either participating or not participating in the national DCT system (art. 60a, 3). The legislation also specifies that data concerning users may only be stored on users' mobile phones (art. 60a.5,b); that geolocation data may not be collected (art. 60a.5,c); that data be deleted as soon as they are no longer useful for contact-tracing purposes (art. 60a.5,d); and that the source code and all technical specifications of the system be made public (art. 60a.5, e). In parallel to these provisions, the Swiss Government issued specific guidance in the form of an ordinance defining basic operational procedures, as well as the procedures following a notification of an encounter with a positive case (818.101.25). The Swiss app, called SwissCovid, was launched on June 25, 2020.[14]

Australia

In late April 2020, **Australia** released its DCT app called CovidSafe, which detected proximal contacts via Bluetooth. The Australian app was based on a system developed in Singapore that was made available as an open-source solution. Australia adopted a data protection approach to governing its DCT app, and in May 2020, the Australian Parliament enacted an amendment to the Privacy Act of 1998 to support the COVIDSafe app.[15] This Amendment introduced novel legal definitions related to DCT and extended privacy-related safeguards to data types and data collection activities specific to DCT. The Amendment also specified a number of data-related activities as serious criminal offences, including unauthorized data collection through DCT, unauthorized use or disclosure of COVID app-collected data; uploading data without consent, moving data collected through the app to locations outside of the country, decrypting encrypted data, and requiring participation in the DCT system by employers (94A). The amendments define app data as "personal information" and extend the authority of the data protection commissioner to allow assessments and investigations related to the app (94A).

United States

Unlike the other countries included in this study, the **United States** did not develop a nationwide DCT app and did not enact DCT-specific laws or regulations at the federal level. Instead, a number of state and local governments developed and released official DCT apps, sometimes with guidance from Apple and Google. By December 2020, twenty states, plus Puerto Rico and the District of Columbia, had released official GAEN apps, and as of July 2022, sixteen states were still using GAEN apps.[16] In addition, three states released non-GAEN apps, described as "location diaries," that collect and store location data on users' phones, which data can then be voluntarily shared with a public health agency if the user subsequently tests positive.[17] This state-by-state approach created gaps in coverage and a lack of interoperability across state borders.[18]

A number of existing federal privacy laws could apply to the use and dissemination of data collected through DCT apps, including laws related to data security, health information, labor and employment, consent, and anti-discrimination.[19] Constitutional privacy protections may also be relevant to DCT technology, particularly if information collected by DCT apps were accessible to law enforcement.[20] But none of these federal laws reference digital contact tracing technology, and as of August 2022, none were updated in response to COVID-19.

Members of the U.S. Congress introduced four bills that would have created specific privacy protections for users of DCT apps,[21] but as of November 2022, none of these bills has been passed by either chamber. A number of U.S. states enacted legislation regulating traditional contact tracing in response to COVID-19, but as of August 2022, only Kansas and Oregon had enacted a law that specifically restricts the collection and use of data collected digitally for contact-tracing

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

purposes.[22] The Kansas law itself is not expansive regarding DTC; it simply prohibits the use of cell phone location data for contact-tracing purposes.[23] The Oregon law prohibits organizations from collecting, using, or disclosing personal health data without revokable, express consent from individuals, and specifies that such consent may not be obtained through a user interface that has been designed to trick users. Additionally, it specifies that contact tracing data cannot be used for commercial advertising or marketing algorithms. The legislatures in some other States, including California, Minnesota, New Jersey, New York, and Ohio, also introduced bills that would also regulate use of DCT apps, but none have become law.[24]

1.2 The Emergency Response Model

The remaining countries in our study adopted a very different approach to DCT governance, which we describe as the "Emergency Response Model." The governments that adopted this model relied on emergency response laws in order to engage in larger-scale data collection than those that adopted the Data Protection Model. Rather than data minimization, the Emergency Response Model focuses on maximizing the public health benefits of DCT through the collection of vast quantities of personal location data stored in a centralized database accessible to the government.

South Korea

South Korea is a paradigmatic example of a country that authorized the development and use of DCT technology on the basis of emergency response laws. The South Korean government relied on its emergency response law to authorize a "network-based approach" to DCT that collects individual user data, including location data, directly from mobile phone networks (as well as other digital sources), and stores these data in a centralized database for ease of contact tracing and other public health interventions. South Korea's DCT system was authorized under the Infectious Disease Control and Prevention Act (IDCPA), which provides for the Korean Center for Disease Control and Prevention (KCDC) to collect personal information necessary to control the spread of infectious diseases.[25] Under this law, the government is authorized to collect personally identifiable network information about users directly from mobile network operators, including location data. The data collection authorized by the IDCPA falls within a standing public health emergency carve-out from South Korea's typical digital privacy law.[26]

On April 2, 2020, in response to COVID-19, the President Moon Jae-In relied on this law to issue an enforcement decree authorizing the collection and storage of additional personal data to track the spread of SARS-CoV-2.[27] The presidential decree authorizes the collection of data including credit card data, transportation records, and image data captured from security cameras.[28] In accordance with the IDCPA and the presidential decree, the South Korean government has collected information about persons who tested positive for SARS-CoV-2 as well as suspected close contacts directly from mobile network providers, banks, and other sources. Data collection was compulsory in the sense that data may be collected without the consent or even the active participation of the individual mobile phone user. Personalized information from these various sources was then collected and stored in a centralized government system called the Epidemic Investigation Support System (EISS). The Ministry of Health collected these data in a centralized database and used them to track the past movement of people who tested positive for COVID-19, using this information for contact tracing and as a basis for imposing quarantine.[29]

Ghana

Similar to South Korea, **Ghana** utilized an emergency provision to authorize centralized network-based data collection in order to aid in the government's contact-tracing efforts. On March 23, 2020, President Nana Addo Dankwa Akufo-Addo issued Executive Instrument 63 (E.I. 63), known as the Emergency Communications System Instrument, 2020, which requires mobile phone network operators and service providers to make available to the government information about mobile phone users, including cell-site location data and location logs, for the purposes of contact tracing.[30] The president's authority to issue E.I. 63 was based on Section 100 of the Electronic Communications Act (ECA) of 2008, which provides that "operators or providers of electronic communications networks or services" must, if required by an executive instrument, "provide any user information or otherwise [*sic*] in aid of law enforcement or national security."[31] The provision of network data by the government under E.I. 63 is compulsory and individual mobile phone users may not opt out of the government's collection of their data from network operators.

On April 13, 2020, not long after the president issued E.I. 63, Vice President Dr. Mahamudu Bawumia announced the launch of an official contact-tracing app, GH COVID-19 Tracker, developed in collaboration with the Ministry of Communications (MoC).[32] The app, which was subsequently updated and relaunched to expand its capabilities, incorporates geofencing and location data, together with QR code

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

check-in functionality, to aid in contact tracing, identify COVID-19 "hotspots," and manage event capacity in compliance with government-mandated guidelines and restrictions.[33] Although downloading the app was voluntary, the app is only a secondary method of data-collection designed to accompany the mandatory collection of data directly from mobile phone network operators.

South Africa

South Africa provides another example of the Emergency Response Model. As in South Korea and Ghana, the initial authorization for DCT in South Africa was pandemic-response authority held by the executive branch. On March 18, 2020, the South African Minister of Cooperative Governance and Traditional Affairs issued COVID-specific regulations as authorized by Section 27(2) of the Disaster Management Act (57/2002). These regulations provide, among other things, that any government minister may "take any [] steps that may be necessary to prevent an escalation of the national state of disaster."[34] Pursuant to this provision, on April 4, 2020, the Information Regulator issued a "Guidance Note on the Processing Of Personal Information In The Management And Containment Of Covid-19 Pandemic," in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA).[35] Among other things, this guidance document requires, under certain conditions, electronic communication service providers to provide the Government with mobile phone-based location data of individual users in order to "manage[] the spread of COVID-19." (5.1)

On April 29, 2020, the Minister of Cooperative Governance and Traditional Affairs issued another set of regulations under the Disaster Management Act providing for the creation of a "COVID-19 Tracing Database," a centralized system designed to collect and store personalized information about all individuals who have been tested for COVID-19 as well as known or suspected contacts of those who tested positive.[36] These regulations and policy documents explicitly authorize the government to collect the location data of individuals who are known or reasonably suspected to have contracted COVID-19, and of the persons with whom they have been in contact, directly from any electronic service provider.[37] The regulation strictly limits the use of these data to government contact-tracing purposes,[38] but individuals have no opportunity to opt out of the collection or use of their data.[39]

Then, on September 2, 2020, the South African government released a new DCT app, called COVID Alert SA, based on the decentralized GAEN protocol.[40] The new app was presented as privacy-preserving and as an effective way to protect public health in the course of the pandemic. Notably, however, this app supple-

Table 1

Country	Name of DCT System	Authorizing Legislation or Policy	Date of Authorizing Legislation or Policy
Australia	COVIDSafe app	Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020	May 15, 2020
France	StopCovid app	Décret n° 2020-650	May 29, 2020
Ghana	Unnamed data collection system	Executive Instrument 63	March 23, 2020
Israel	SIGINT Oversight System	Resolution 4916	March 24, 2020
Italy	Immuni app	GPDP authorization for the Covid-19 Alert System, n. 95	June 1, 2020
South Africa	COVID-19 Tracing Database	Regulations Issued under Section 27(2) of the Disaster Management Act	April 29, 2020
South Korea	Epidemic Investigation Support System (EISS)	Enforcement Decree of The Infectious Disease Control And Prevention Act, Presidential Decree No. 30596	April 2, 2020
Switzerland	SwissCovid	Amendment to Epidemics Act of 2012 (AS 2020 2191)	June 19, 2020
United States	No national DCT system	No national DCT legislation	N/A

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

Table 2

	Data minimization	Large-scale data collection
DCT authorized under data protection law	France Italy Australia Switzerland	N/A
DCT authorized under emergency response law	N/A	South Korea Ghana South Africa Israel

mented — but did not replace or eliminate — the government's ability to collect user data directly from mobile phone network operators and to store these data in the centralized COVID-19 Tracing Database.[41]

Israel

Finally, much like South Africa, **Israel** employed a two-pronged approach, including both a voluntary public-facing app and large-scale data collection directly from mobile phone networks. Israel provides a distinctive example of the Emergency Response Model, as Israel authorized its DCT under its national security law, as opposed to public health laws. Specifically, the more intrusive aspects of Israel's DCT system were authorized under Sections 38 and 39 of the Basic Law of the Government of Israel, which grants far-reaching powers for declaring a state of emergency, including the temporary suspension of any existing statute.[42]

In March 2020, The Israeli Government issued Resolution 4916, which commissioned the Israeli Security Agency (ISA), Israel's domestic security agency — also known as the Shin-Bet, "Shabak", or General Security Service (GSS) — to collect data from mobile phones for digital contact tracing.[43] The government expressed its commitment to limited data collection, including no recording of phone calls or text messages, and also promised to delete all information once the COVID-19 pandemic ended.[44] However, the technology deployed by the ISA, the SIGINT Oversight system also known as "the Tool," collected personal cell-site location data based on mobile phone caches, which was then cross-referenced with the locations of individuals who tested positive for COVID-19.[45] This personalized location information allowed the ISA to identify the names and contact information of individuals who were in the same location as those who tested positive during likely periods of transmissibility. The Ministry of Health could then use this information to contact people who may have been exposed to the coronavirus, often requiring them to quarantine and register with the Ministry of Health's database.[46] The Ministry of Health also released a downloadable app, called HaMagen, to facilitate its communication process.[47] As in South Africa, however, this app augmented, but did not replace, the government's compulsory centralized data collection process.

2. Discussion

As described above, our research revealed a stark dichotomy between two key DCT governance models adopted by the countries included in our survey. (See Table 2.) The countries that prioritized individual privacy in adopting their DCT systems — namely, Italy, France, Australia, and Switzerland — adhered to principles of data minimization and privacy by design.[48] These countries adopted legislative interventions specifically aimed at linking DCT to privacy and data protection provisions and created strict limits on data collection, storage, and analysis for DCT purposes (privacy-by-default). Moreover, all of these countries embedded technological safeguards such as anonymization and data-minimization in their DCT systems — e.g. the collection of Bluetooth proximity data, not location data (privacy-by-design). Finally, in all of these countries, DCT was app-based and the use of DCT was voluntary, with digital monitoring limited to those who chose to download and install the app onto their phone.

On the other hand, the countries that authorized their DCT systems under emergency response laws — namely, South Korea, Ghana, South Africa, and Israel — allowed for the collection of users' location data directly from mobile phone network operators, without requiring the consent or cooperation of users.

Both models of DCT governance are premised on the assumption that widespread adoption of DCT can substantially boost virus containment efforts (in conjunction with other measures). Given the impor-

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

tance of boosting uptake, we believe that a number of important lessons can be learned about the governance of digital technologies for public health based on these contrasting governance approaches to DCT technology during the first year of the COVID-19 pandemic.

2.1 The Data Protection Model Emphasizes Individual Risk Over Collective Benefit

The Data Protection Model attributes a pivotal role to protecting user privacy, and advocates of this model assert that increasing use of DCT is largely a function of addressing legitimate privacy concerns on the part of the population. However, although the Data Protection Model was intended to address privacy concerns and thus to drive widespread uptake of DCT systems among citizens, the actual level of uptake of such systems failed to meet expectations and was insufficient to generate its intended public health impact. For this reason, although emerging studies continue to demonstrate the impact of DTC in the pandemic, the effort to use DCT apps governed by the Data Protection Model has been publicly perceived as a failure, especially in Europe.[49]

In many countries that employed the Data Protection Model, privacy-related risks have been at the forefront of the public debate about DCT. Studies have shown that the media's emphasis on privacy concerns — coupled with uncertainty about the effectiveness of DCT — may have materially undermined public trust and interest in the new technology. For example, an analysis of newspaper coverage of DCT apps in Germany, Austria, and Switzerland suggests that an emphasis on "debates surrounding data protection, privacy, and voluntariness" together with characterizing the use of DCT as controversial, may have caused members of the public to be reluctant and cautious about using DCT.[50] Similarly, in the United States, polling shows that State governments considered privacy risks to be a barrier to implementing the new app-based or mobile phone-based technology to respond to the pandemic.[51]

It is possible that individuals therefore reacted to the adoption of the Data Protection Model by seeing it as a reason to avoid using DCT, not an assurance of its safety. Individuals have grown increasingly wary of digital technology's capacity to collect personal data without their knowledge or consent. And a legislative approach focused on data protection in the context of data-collection technology generally signals the potential privacy risks of such technology. Lending credence to these concerns, it was reported that the Australian national intelligence agency was able to access data collected by its national DCT app, despite comprehensive legal protections intended in part to prevent this from happening.[52]

In addition, individuals may have been wary of the central role that private companies, especially Apple and Google, played in DCT development and governance. Largely because of the need for rapid DCT deployment, some countries, such as Italy and the United States, relied on private sector providers for both the API and the actual development of their DCT apps. France, by contrast, developed its DCT app in-house, in order to avoid relying on the GAEN system.[53] In addition, some scholars have suggested that Google and Apple sought self-interested while at the same time presenting themselves as more credible "champions of privacy than some democratic governments."[54] It is clear that these companies stepped in at an early stage to design a DCT system that protects the privacy of the app users by limiting the types and uses of data collected, sometimes at the cost of public health utility.[55] In the UK for instance, Apple and Google prevented an update of the NHS DCT app that would have enabled users to be notified in case their log of locations (generated as they check-in in venues by scanning QR codes with the app) matched a list of venues considered as potential virus hotspots.[56] Moreover, researchers involved with the development of the NHS app have argued that an ability to evaluate the effectiveness of DCT systems is essential to their application going forward, necessitating the collection of data, including location data, that is not allowed by the GAEN system.[57]

Arguably, the influence exerted by Apple and Google undermined the benefits of DCT for public health protection. Given the ongoing international debate about the excessive power accumulated by unaccountable tech giants, it is not surprising that governments' reliance on Google and Apple in a matter of public interest and common concern may have alienated at least some potential DCT users. This effect should not be attributed to the lack of public trust in corporations such as Apple and Google.[58] Rather, the delegation of governance prerogatives to tech giants may have reinforced currents of public distrust in the capacity of governments to adequately handle the response to the COVID-19 emergency, specifically as to the use of novel digital health solutions.[59] The reliance on public/private partnerships should be evaluated to protect against loss of public trust and engagement in a DCT effort.

It appears that the public health purpose for using DCT was eclipsed in many countries by the Data Protection Model's emphasis on individual privacy.

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

Empirical studies have shown that members of the public cite lack of perceived benefit as the main reason for not using DCT apps,[60] which in turn is reflected in a widespread media discussion of such systems having unclear benefit. In a pandemic, another message may therefore need to be communicated along with the information-protection message of the Data Protection Model. Individuals may be willing to take on sacrifices or inconveniences to help out their community in responding to a pandemic. This claim is supported by empirical studies showing that while privacy concerns nurture skepticism towards the use of DCT, the prospect of contributing to the "greater good" motivates people to embrace such use.[61] Indeed, extensive surveys conducted in Europe suggest that even those who value privacy are also motivated by a variety of values in this context, including protecting the health of their community. This suggests that DCT might have gained greater public acceptance if it had been more clearly presented as a public health intervention whose use would allow individuals to contribute to fighting the pandemic.

In employing the Data Protection Model of governance, many European governments, almost certainly influenced by the GDPR, may have failed to tap into their citizens' motivations to help protect the health of their fellows and their community by accepting fewer privacy protections.[62] Rather than creating governance mechanisms to build public trust and transparency about the functionality and potential benefits of the DCT apps, those governments focused on privacy safeguards such as data-minimization. At least arguably, this limited the public-health utility of DCT by reducing the quantity and types of valuable data to which public health officials had access. For example, the GAEN approach, employed in the United States and in much of Europe, collects only anonymized proximity data, stored in decentralized fashion on users' phones. In contrast, the use of less privacy-preserving approaches, such as collecting location or proximity data in a centralized database to which public health authorities have access, enables a more granular tracking of positive cases.

Effective governance of DCT will likely require a public justification based on the potential benefit to the community of widespread adoption of the technology. Even if other forms of public justification are employed — e.g., direct communication from the public health agencies — a narrow focus on individual privacy protection is arguably incompatible with the public health value of DCT. DCT requires a governance approach that builds public trust, premised on adequate safeguards, dedicated oversight bodies to deter data misuse on the part of both private-sector actors and governments,[63] and transparency about evidence-based objectives and the expected contribution of the technology to combatting a public health emergency like the COVID-19 pandemic.[64]

To summarize, the Data Protection Model has a number of limitations when applied to DCT governance. Most importantly, its prioritization of user privacy tends to limit data collection, as well as data analysis, sharing, and use, and so may reduce the public health utility of DCT. And ironically, by emphasizing privacy as a concern, the Data Protection model may undermine or conflict with the government's efforts to motivate uptake of DCT. Ideally, a governance approach that is well suited to DCT should be able to determine the appropriate privacy protections in light of public values, democratic deliberation, and changing facts on the ground, and to communicate the potential of DCT to protect human life in a widespread pandemic.

2.2 The Emergency Response Model Raises Concerns about Excessive Government Surveillance

In contrast with the Data Protection Model, the Emergency Response Model allowed governments to prioritize the collection of data for public health purposes over protecting the privacy of user data. For example, research suggests that South Korea's comprehensive network-based DCT system may have helped to limit the spread of SARS-CoV-2.[65] Similarly, Ghana's contact tracing system (which includes both digital and traditional data collection), together with its significant testing capacity, may have contributed to the country's promising public health outcomes.[66]

Authorizing DCT technology under emergency response powers, however, raises significant concerns about government surveillance and unchecked governmental authority. In particular, the collection of personal information necessary for effective DCT raises serious risks of government misuse of data and invasion of privacy. In South Korea, for example, concerns were raised by scholars and civil rights groups that the government has overused this system to collect information pertaining to more individuals than strictly necessary to respond effectively to the pandemic, and that, in particular, the government's large-scale data collection techniques violated constitutional rights protections.[67]

In Israel, human rights groups brought legal challenges against the government's DCT surveillance system, resulting in the Israeli Supreme Court overturning the initial emergency justification of DCT and requiring legislative approval.[68] In light of these

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

challenges, and citing the lack of parliamentary oversight and disproportionate infringement on the right to privacy, the Israeli government decided to repeal the emergency orders, switching the foundation of ISA surveillance powers to the ISA Security Law.[69] However, the Supreme Court later held this interpretation of the ISA Security Law to be illegal, ruling that involving the ISA in COVID-19-response measures would require legislative efforts.[70] Shortly after, in July, 2020, the Knesset enacted a law authorizing the ISA to collect identifiable mobile phone data from individuals who have tested positive for Sars-CoV-2, and to provide the Ministry of Health with their location data and the identity of their close contacts.[71]

In Ghana, a number of scholars argued that President Akufo-Addo exploited the COVID-19 crisis to bolster his power at the expense of transparency, accountability, and civil rights.[72] Some legal scholars argued that because E.I. 63 authorizes the collection of network-based data of all mobile phone users, it raises significant concerns about invasion of privacy and abuse of power and may be inconsistent with the spirit of Section 100 of the ECA.[73] Others argued that E.I. 63 is unconstitutional on the ground that the president has not declared an official State of Emergency, as provided under articles 31 and 32 of the 1992 Constitution, as well as the Emergency Powers Act 1994 (Act 472).[74] Declaring an official State of Emergency would provide a sound constitutional basis for many of President Akufo-Addo's pandemic-response policies, but would also subject them to the oversight of Parliament and other governmental bodies.[75] Instead of declaring a State of Emergency, the president imposed restrictions and other pandemic responses under the recently enacted Imposition of Restrictions Act, which has also prompted significant criticism from legal scholars and civil rights advocates.[76]

Responding to these concerns, some have argued that, in countries such as South Korea, public acceptance of DCT was largely due to the government's concerted communications about the expected public benefits of the technology.[77] It is difficult to verify public acceptance of a compulsory network-based surveillance system that left no opportunity for citizens to opt-out. It does seem, however, that the South Korean public was aligned with the government's public health goals; the fact that certain measures are mandatory does not rule out that they are voluntarily supported by public trust, as in the case of mandatory use of seatbelts, for instance.

The collection by the government of enormous amounts of personal data via mobile phones, as occurred in the countries that adopted the Emergency Response Model, is a risk that must be evaluated in context. Emergency response authority may be an effective tool for responding to a pandemic situation. Governments must act fast, and flexibly, to respond to a rapidly changing public health crisis, and formal procedures of law and policy-making are sometimes inadequate to that task. It would, therefore, be misguided to criticize all forms of emergency response just because they do not employ traditional mechanisms of oversight, accountability, and public participation. However, the legitimacy of the use of exceptional state powers in the context of the exceptional circumstances of the COVID-19 pandemic has been a matter of significant debate, and the government's collection and use of personal data collected via mobile phones, raises novel ethical questions, even where the goal is the protection of public health.

In short, authorizing DCT under an Emergency Response governance model risks excessive government surveillance and the infringement of civil liberties. Without adequate oversight safeguards, DCT technology may be used by the government to collect extensive amounts of personally identifiable data, raising fears about intrusive forms of surveillance that could extend beyond public health necessities.

The contrasting governance approaches adopted for "first generation" DCT can teach us important lessons about the future governance of DCT. We must learn from both governance models — Data Protection and Emergency Response — in order to develop a new governance approach that is able to guide the ethical and effective use of DCT and related digital public health technology going forward. Ultimately, the effective governance of DCT may help end the COVID-19 pandemic and to prepare for and combat potential infectious disease outbreaks in the future.

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

Conclusion

Our research shows that in the countries surveyed, DCT systems were accompanied by one of two distinct models of governance, each of which has critical limitations. First, the Data Protection Model was not ideally suited to digital public health interventions such as DCT, because it tended to prioritize user privacy in a situation where, unlike commercial transactions, human lives are at stake. By emphasizing privacy concerns rather than the critical need to collect personal data to prevent widespread infection, the Data Protection Model may have undermined uptake of DCT. The Emergency Response Model, on the other hand, often lacked adequate oversight, accountability, and privacy protections. Although this approach may promise greater public health utility, especially if it involves a more data-intensive DCT system, it raises serious questions of legitimacy and justification absent an adequate governance and oversight infrastructure.

Effective and ethical use of DCT going forward requires incorporation of traditional governance values, including accountability, transparency, and public participation. The emergency context should not prompt governments to abandon these values; but at the same time, these values cannot be adequately realized (or replaced) by special features of the design of the technology itself.

A new governance approach is arguably required for designing and implementing DCT technology going forward. Much like traditional contact tracing, DCT must be explained and "marketed" to individuals in terms of civic responsibility, solidarity, and collective action. This objective can be achieved through transparent governance, enabling the public to know what impact governments expect DCT to have in containing the spread of the virus, and what levels of individual participation, including personal data-sharing, would be required to meet those expectations.

The contrasting governance approaches adopted for "first generation" DCT can teach us important lessons about the future governance of DCT. We must learn from both governance models — Data Protection and Emergency Response — in order to develop a new governance approach that is able to guide the ethical and effective use of DCT and related digital public health technology going forward. Ultimately, the effective governance of DCT may help end the COVID-19 pandemic and to prepare for and combat potential infectious disease outbreaks in the future.

Note

The study described in this article was commissioned and partly funded by the World Health Organization (WHO). Copyright in the original work on which this article is based belongs to WHO. The authors have been given permission to publish this article. The authors alone are responsible for the views expressed in this publication and they do not necessarily represent the views, decisions or policies of the WHO. Additional funding was provided by the Swiss National Science Foundation (NRP77 grant 407740_1873560). BH reports support from the Hecht-Levi Postdoctoral Fellowship. RGA reports support from the Oxford-Johns Hopkins Global Infectious Disease Collaborative, funded by the Wellcome Trust (grants numbers 221719 and 216355), and partial support from the Zuckerman-CHE STEM Leadership Program. Additional research support was provided by Arnold & Porter Kaye Scholer LLP, and by Shannon Hubbs, Antonis Kouris, and Renan Leonel at ETH. Dr. Vayena reports grants from the Swiss National Science Foundation, during the conduct of the study; personal fees from IQVIA, personal fees from Roche Diagnostics, outside the submitted work; and service as Chair of the Greek National Bioethics and Technoethics Committee. Ms. Perkins reports grant funding from Google, outside the submitted work.

References

1. L. Ferretti, et al., "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing," *Science* 368, no. 6491 (2020): eabb6936; M. Kendall, et al., "Epidemiological Changes on the Isle of Wight after the launch of the NHS Test and Trace Programme: A Preliminary Analysis," *The Lancet Digital Health* 2, no. 12 (2020): e658-e666; C. Wymant, L. Ferretti, D. Tsallis, et al., "The Epidemiological Impact of the NHS COVID-19 App," *Nature* 594 (2021): 408–412, https://doi.org/10.1038/s41586-021-03606-z; D. Lewis, "Contact-Tracing Apps Help Reduce COVID Infections, Data Suggest," *Nature* 22 (2021); J. O'Connell and D. T. O'Keeffe, "Contact Tracing for Covid-19 — A Digital Inoculation Against Future Pandemics," *New England Journal of Medicine* 385, no. 6 (2021): 484-487.
2. L. White and P. van Basshuysen, "Without a Trace: Why did Corona Apps Fail?" *Journal of Medical Ethics* 47, no. 12 (2021), doi: 10.1136/medethics-2020-107061; F. Vogt et al., "Effectiveness Evaluation of Digital Contact Tracing for COVID-19 in New South Wales, Australia," *The Lancet Public Health* 7, no. 3 (2022): e250-e258.
3. D. Klinkenberg, C. Fraser, and H. Heesterbeek, "The Effectiveness of Contact Tracing in Emerging Epidemics," *PloS One* 1, no. 1 (2006): e12.
4. See, e.g., the Flu Near You app, *available at* <https://flunearyou.org/#!/> (last available at Nov. 22, 2022).
5. Directorate-General for Justice and Consumers, European Commission, "Communication from the Commission: Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection. 2020 O.J. (C 124) I/01 (EC)," *available at* <https://op.europa.eu/en/publication-detail/-/publication/f8f4dc8b-80a4-11ea-bf12-01aa75ed71a1/language-en> (last visited Nov. 22, 2022).
6. Regulation 2016/679 (General Data Protection Regulation), 2016 O.J. (L119) 1 (EU).
7. Apple, Google. Exposure Notifications: Frequently Asked Questions v1.2. (September 2020), *available at* <https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf> (last visited Nov. 22, 2022).
8. Misure urgenti per la funzionalita' dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonche' disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19. Presidential Decree-Law, 30 April 2020, n. 28 (GU Serie Generale n.111 del 30-04-2020) (It.), available at <https://www.gazzettaufficiale.it/eli/id/2020/04/30/20G00046/sg> (last visited Nov. 22, 2022).
9. Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19- App Immuni. Official Guidance, June 6, 2020 (It), *available at* <https://www.garanteprivacy.it/web/guest/home/docweb/-/

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

docweb-display/docweb/9356568> (last visited Nov. 22, 2022).
10. The list includes, among others, the Data Protection Authority (Commission National de l'Informatique et des Libertés — CNIL), the National Council on Digital Affairs (Conseil National du Numérique — CNNum) and the National Pilot Committee on Digital Ethics (Comité National Piloted'Éthique du Numérique — CNPEN).
11. Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé "StopCovid," Ministry of Social Affairs and Health Directive, 29 May 2020 (Fr.), *available at* <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041936881/> (last visited Nov. 22, 2022).
12. Ministère de l'économie des finances et de la relance, "L'application StopCovid est disponible au téléchargement dans les magasins d'applications," Ministry of the Economy, Finance and Recovery Directive, June 2, 2020 (Fr.), *available at* <https://www.economie.gouv.fr/appli-stop-covid-disponible> (last visited Nov. 23, 2022).
13. Gouvernement Français, "Projet STOPCOVID," Dossier de presse, May 21, 2020, *available at* <https://decryptageo.fr/wp-content/uploads/2020/05/Dossier-de-presse-Pojet-StopCovid.pdf> (last visited Nov. 23, 2022).
14. P. Daniore, et al., "The SwissCovid Digital Proximity Tracing App After One Year: Were Expectations Fulfilled?" *Swiss Medical Weekly* 151, no. 3636 (2021): w30031.
15. "Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020 (Australia), *available at* <https://www.legislation.gov.au/Details/C2020A00044> (last visited Jan. 10, 2023). See also G. Goggin, "COVID-19 Apps in Singapore and Australia: Reimagining Healthy Nations with Digital Technology," *Media International Australia* 177, no. 1 (2020): 61-75.
16. State Approaches to Contact Tracing during the COVID-19 Pandemic, National Academies of State Health Policy, Jul. 7, 2022, *available at* <https://www.nashp.org/state-approaches-to-contact-tracing-covid-19/> (last visited Nov. 23, 2023).
17. M. Sato, "Contact Tracing Apps Now Cover Half of America. It's Not Too Late to Use One," *MIT Technology Review*, December 14, 2020, *available at* <https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/> (last visited Nov. 23, 2022).
18. D. Ramjee, P. Sanderson, and I. Malek, "COVID-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance," *Cardozo Law Review* 100 (2021): 108–111, *available at* <http://cardozolawreview.com/covid-19-and-digital-contact-tracing-regulating-the-future-of-public-health-surveillance> (last visited Nov. 23, 2022).
19. See the "Legal Consideration" in *Digital Contact tracing for Pandemic Response: Ethics and Governance Guidance*, ed. J.P. Kahn (Johns Hopkins University Press: 2020), *available at* <https://muse.jhu.edu/book/75831> (last visited Nov. 23, 2022). See also N. Ram and D. Gray, "Mass Surveillance in the Age of COVID-19," *Journal of Law and the Biosciences* 7, no. 1 (2020): lsaa023.
20. A. Z. Rozenshtein, "Digital Disease Surveillance," *American University Law Review* 70, no. 5 (2021): 1511-1576.
21. Congressional Research Service, "Digital Contact Tracing and Data Protection Law," R46542, September 24, 2020, *available at* <https://crsreports.congress.gov/product/pdf/R/R46542> (last visited Nov. 23, 2022).
22. Kan. Stat. Ann. § 48-961 "COVID-19 contact tracing privacy act."
23. 2021 Oregon Laws Ch. 305 (H.B. 3284).
24. AB-1782 Personal Information: Contact Tracing., CAL. LEGIS, *available at* <https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200AB1782> (last visited Aug. 3, 2022); HF 164, MINN. LEGIS., *available at* <https://www.revisor.mn.gov/bills/bill.php?view=chrono&f=HF%20164&y=2020&ssn=1&b=house#actions> (last visited Aug. 3, 2022); New Jersey Assembly Bill 4170, LEGISCAN, *available* at <https://legiscan.com/NJ/bill/A4170/2020> (last visited Aug. 3, 2022) (the bill's text is also *available at* <https://pub.njleg.gov/bills/2020/A4500/4170_R1.HTM> (last visited Nov. 28, 2022)); Senate Bill S8450C, N.Y . ST A TE S., *available at* <https://www.nysenate.gov/legislation/bills/2019/s8450/amendment/c> (last visited Aug. 3, 2022); House Bill 61, OHIO LEGIS., *available at* <https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA133-HB-61> (last visited Aug. 3, 2022).
25. Infectious Disease Control and Prevention Act (IDCPA) Art. 76-2 (S. Kor.) (authorizing data collection for public health response to infectious disease). Data regarding travel region, time and other related medical information can be collected by the director of (regional) quarantine stations pursuant to the Quarantine Act (Act no. 15266, Dec. 19, 2017).
26. Collection of data relevant to COVID-19 response falls under the partial exclusion of application of the Personal Information Protection Act (PIPA) Chapter 9 Article 58(1) 3 (S. Kor.). See also, S. Park, E. Cho, "National Infectious Diseases Surveillance Data of South Korea," *Epidemiology and Health* 36 (2014): e2014030, doi:10.4178/epih/e2014030.
27. Enforcement Decree Of The Infectious Disease Control And Prevention Act, Presidential Decree No. 30596, April 2, 2020 (S. Kor.), *available at* <https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=1&query=ENFORCEMENT+DECREE+OF+THE+INFECTIOUS+DISEASE+CONTROL+AND+PREVENTION+ACT#liBgcolor0> (last visited Nov. 28, 2022).
28. A. Roussi, "The South Korean Government Reportedly uses Facial Recognition Technology to Identify Persons Captured by Security Cameras," *Nature*, November 18, 2020, *available at* <https://www.nature.com/articles/d41586-020-03188-2> (last visited Nov. 28, 2022).
29. Y. J. Park et al., "Development and Utilization of a Rapid and Accurate Epidemic Investigation Support System for COVID-19," *Osong Public Health Research Perspectives* 11, no. 3 (2020): 118.
30. Executive Instrument 63 (E.I. 63) (March 23, 2020) (Ghana), *available at* <https://ghanalawhub.com/wp-content/uploads/2020/04/E.I.-63.pdf> (last visited January 10, 2023).
31. Electronic Communications Act, 2008 (Act 775) (Ghana) Section 100, *available at* <https://www.moc.gov.gh/sites/default/files/downloads/Electronic%20Communications%20Act-775.pdf> (last visited Nov. 28, 2022).
32. Ministry of Communications, "Launch of GH COVID-19 Tracker App," *available at* <https://www.moc.gov.gh/launch-gh-covid-19-tracker-app> (last visited Nov. 28, 2022).
33. Graphic Online, "Ghana's COVID-19 Tracker App Upgraded," September 2, 2020, *available at* <https://www.graphic.com.gh/news/general-news/govt-re-launches-covid-19-tracker-app.html> (last visited Nov. 28, 2022).
34. Regulations Issued in terms of Section 27(2) of the Disaster Management Act, 2002 (18 March 2020) (S. Afr.) Section 10(8)(c), *available at* <https://www.gov.za/sites/default/files/gcis_document/202003/43107gon318.pdf> (last visited Nov. 28, 2022).
35. Guidance Note On The Processing Of Personal Information In The Management And Containment Of Covid-19 Pandemic In Terms Of The Protection Of Personal Information Act 4 Of 2013 (POPIA) (S. Afr.), *available at* <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf> (last visited No. 28, 2022).
36. Regulations Issued in terms of Section 27(2) of the Disaster Management Act, 2002 (29 April 2020) (S. Afr.) Section 8, *available at* <https://www.gov.za/sites/default/files/gcis_document/202004/43258rg11098gon480s.pdf> (last visited Nov. 28, 2022).
37. *Id.* Section 8(10).
38. *Id.* Section 8(11).
39. *Id.* Section 8(10).
40. South African Government News Agency, "Health Launches COVID-19 Contact Tracing App," September 2, 2020, *available at* <https://www.sanews.gov.za/south-africa/health-

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

launches-covid-19-contact-tracing-app> (last visited Nov. 28, 2022).
41. M. Viljoen, et al., "Contact Tracing During the COVID-19 Pandemic: Protection of Personal Information in South Africa," *South African Journal of Bioethics and Law* 13, no. 1 (2020): 15-20, *available at* <http://www.sajbl.org.za/index.php/sajbl/article/view/626/620> (last visited Nov. 28, 2022).
42. The Israeli Government (Knesset), Public Health Ordinance (1940) (Isr.), *available at* <https://www.gov.il/en/departments/legalInfo/public_health_ordinance_1940> (last visited Nov. 28, 2022).
43. Authorization of the General Security Service to assist in the national effort to reduce the spread of the new corona virus] Resolution number 4916, March 24, 2020 (Isr.), *available at* <https://www.gov.il/he/departments/policies/dec4916_2020> (last visited Nov. 28, 2022) Note that the ISA acts in full and total secrecy as established in the ISA Security Law of 2002.
44. T. Shwartz Altshuler and R. Aridor Hershkovitz, "Digital Contact Tracing and the Coronavirus: Israeli and Comparative Perspectives," Foreign Policy at Brookings (2020), *available at* <https://www.brookings.edu/wp-content/uploads/2020/08/FP_20200803_digital_contact_tracing.pdf> (last visited Nov. 28, 2022).
45. See A. Cahane, "Israel's SIGINT Oversight Ecosystem: COVID-19 Secret Service Location Tracking as a Test Case," *University of New Hampshire Law Review* 19, no. 2 (2021): 451-490, *available at* <http://dx.doi.org/10.2139/ssrn.3748401> (last visited Nov. 28, 2022).
46. T. S. Altshuler and R. A. Hershkovitz, "How Israel's COVID-19 Mass Surveillance Operation Works," July 6, 2020, Brookings.com, *available at* <https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/> (last visited Nov. 28, 2022).
47. The HaMagen app, *available at* <https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/> (last visited Nov. 28, 2022).
48. L. A. Bygrave, "Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements," *Oslo Law Review* 4, no. 2 (2017): 105-120.
49. "Covid-19 contact tracing apps: a €100m failure," Voxeurop English, *available at* <https://voxeurop.eu/en/covid-19-track-trace-apps-a-100m-failure/> (last visited Nov. 28, 2022).
50. J. Amann, J. Sleigh, and E. Vayena, "Digital Contact-Tracing During the Covid-19 Pandemic: An Analysis of Newspaper Coverage in Germany, Austria, and Switzerland," *Plos One* (2021), *available at* <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0246524> (last visited Nov. 28, 2022).
51. L. Van Ness, "For States' COVID Contact Tracing Apps, Privacy Tops Utility," *Pew Stateline*, March 19, 2021, *available at* <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/19/for-states-covid-contact-tracing-apps-privacy-tops-utility> (last visited Nov. 28, 2022).
52. Z. Whittaker, "Australia's Spy Agencies Caught Collecting COVID-19 App Data," *Tech Crunch*, November 24, 2020, *available at* <https://techcrunch.com/2020/11/24/australia-spy-agencies-covid-19-app-data/> (last visited Nov. 28, 2022).
53. See R. Dillet, "France Releases Contact-Tracing App StopCovid," Techcruch.com, June 2, 2020, *available at* <https://techcrunch.com/2020/06/02/france-releases-contact-tracing-app-stopcovid-on-android/> (last visited Nov. 28, 2022).
54. T. Sharon, "Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers," *Ethics and Information Technology* 23, Supp. 1 (2020): 45-57.
55. R. A. Fahey and A. Hino, "COVID-19, Digital Privacy, and the Social Limits on Data-Focused Public Health Responses," *International Journal of Information Management* 55 (2020): 102181.
56. A. Hern, "Apple and Google Block NHS Covid App Update over Privacy Breaches," *The Guardian*, April 12, 2021, *available at* <https://www.theguardian.com/world/2021/apr/12/apple-and-google-block-nhs-covid-app-update-over-privacy-breaches> (last visited Nov. 28, 2022).
57. V. Colizza, et al. "Time to Evaluate COVID-19 Contact-Tracing Apps," *Nature Medicine* 27, no. 3 (2021): 361-362.
58. C. Newton, "The Verge Tech Survey 2020," *The Verge*, March 2, 2020, *available at* <https://www.theverge.com/2020/3/2/21144680/verge-tech-survey-2020-trust-privacy-security-facebook-amazon-google-apple> (last visited Nov. 28, 2022).
59. S. Altmann, et al., "Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study," *JMIR mHealth and uHealth* 8, no. 8 (2020): e19857; V. von Wyl, et al., "Drivers of Acceptance of COVID-19 Proximity Tracing Apps in Switzerland: Panel Survey Analysis," *JMIR Public Health and Surveillance* 7, no. 1 (2021): e25701.
60. V. Von Wyl, "Challenges for Nontechnical Implementation of Digital Proximity Tracing During the COVID-19 Pandemic: Media Analysis of the SwissCovid App," *JMIR mHealth and uHealth* 9, no. 2 (2021): e25345.
61. S. N. Williams et al., "Public Attitudes towards COVID- 19 Contact Tracing Apps: A UK- Based Focus Group Study," *Health Expect* 24, no. 2 (2020): 377-385; F. Lucivero et al., "Normative Positions towards COVID-19 Contact-Tracing Apps: Findings from a Large-Scale Qualitative Study in Nine European Countries," *Critical Public Health* (2021): 1-14.
62. See: B. Jennings, "Public Health and Civic Republicanism: Toward an Alternative Framework for Public Health Ethics," *Ethics, Prevention, and Public Health*, A. Dawson and M. Verweij, eds. (New York: Oxford, 2007): 30-58.
63. A. Blasimme, A. Ferretti, and E. Vayena, "Digital Contact Tracing Against COVID-19 in Europe: Current Features and Ongoing Developments," *Frontiers in Digital Health* (2021), *available at* <https://doi.org/10.3389/fdgth.2021.660823> (last visited Nov. 28, 2022).
64. A. Blasimme and E. Vayena, "What's Next for COVID-19 Apps? Governance and Oversight," *Science* 370, no. 6518 (2021): 760-762.
65. See Y. Huang, M. Sun, and Y. Sui, "How Digital Contact Tracing Slowed Covid-19 in East Asia," *Harvard Business Review*, April 15, 2020, *available at* <https://hbr.org/2020/04/how-digital-contact-tracing-slowed-covid-19-in-east-asia> (last visited Nov. 28, 2022).
66. J. Zhang, J. Nonvignon, and W. Mao, "How Well is Ghana — with One of the Best Testing Capacities in Africa — Responding to COVID-19?" Brookings, July 28, 2020, *available at* <https://www.brookings.edu/blog/future-development/2020/07/28/how-well-is-ghana-with-one-of-the-best-testing-capacities-in-africa-responding-to-covid-19/> (last visited Nov. 28, 2022); "'Test and trace' has worked for us, Ghana's president says," Reuters, April 29, 2020, *available at* <https://www.reuters.com/article/us-health-coronavirus-ghana/test-and-trace-has-worked-for-us-ghanas-president-says-idUSKBN22B2OE> (last visited Nov. 28, 2022).
67. G. Jung, H. Lee, A. Kim, and U. Lee, "Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea," *Front Public Health* 8 (2020), doi:10.3389/fpubh.2020.00305.
68. Y. Keshet, "Fear of Panoptic Surveillance: Using Digital Technology to Control the COVID-19 Epidemic," *Israel Journal of Health Policy Research* 9 (2020); A. Bryk Silveira, "Digital Tracing and COVID-19 – The Israeli Case," Institute for Internet & the Just Society, April 11, 2021, *available at* <https://www.internetjustsociety.org/digital-tracing-and-covid-19-the-israeli-case> (last visited Nov. 28, 2022).
69. HCJ 2109/20, *Adv. Shahar Ben Maher et al. 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.* For an overview, see A. Sharon, "COVID-19 Roundup," VERSA Opinions of the Supreme Court of Israel, May 27, 2020, Yeshiva University: Benjamin N. Cardozo School of Law, *available at* <https://versa.cardozo.

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)

yu.edu/viewpoints/covid-19-roundup> (last visited Nov. 28, 2022).

70. See Altshuler and Hershkovitz, 2020, *supra* note 46; see also A. Cahane, "Israel Reauthorizes Shin Bet's Coronavirus Location Tracking," Lawfare Blog, July 3, 2020, *available at* <https://www.lawfareblog.com/israel-reauthorizes-shin-bets-coronavirus-location-tracking> (last visited Nov. 28, 2022).
71. Law to Assist in the National Effort to Reduce the Spread of the New Corona Virus (Temporary Order) (Amendment) 5720-20, July 21, 2020 (Isr.), *available at* <https://main.knesset.gov.il/Activity/Legislation/Laws/Pages/LawBill.aspx?t=LawReshumot&lawitemid=2141852> (last visited Nov. 28, 2022).
72. See "Ghana Opposition to Challenge Presidential Loss," Reuters, December 29, 2020, *available at* <https://www.reuters.com/article/us-ghana-election/ghana-opposition-to-challenge-presidential-election-loss-idUSKBN2931P2> (last visited Nov. 28, 2022).
73. J. Asare, "Communications Instrument, 2020 (E.I. 63); A Dangerous Illegality," Ghana Law Hub, May 26, 2020, *available at* <https://ghanalawhub.com/establishment-of-emergency-communications-instrument-2020-e-i-63-a-dangerous-illegality/> (last visited Nov. 28, 2022); "Akufo-Addo using coronavirus as excuse to track your calls and check your wallet – Samson Lardy," Ghana News, *available at* <https://ghananewsonline.com.gh/akufo-addo-using-coronavirus-as-excuse-to-track-your-calls-and-check-your-wallet-samson-lardy/> (last visited Nov. 28, 2022).
74. M. E. Addadzi-Koom, "Quasi-State of Emergency: Assessing the Constitutionality of Ghana's Legislative Response to Covid-19," *The Theory and Practice of Legislation* 8, no. 3 (2020): 311-327. For a legal challenge brought against E.I. 63 on the same grounds, see also: M. Sullemana, "Ghana: Legal Practitioner Sues to Block Release of Personal Info of Subscribers," allAfrica, April 23, 2020, *available at* <https://allafrica.com/stories/202004230919.html> (last visited Nov. 28, 2022).
75. Addadzi-Koom 2020, *supra* note 74.
76. *Id.* See also, K. Appiagyei-Atua, "Ghana's President has Invoked a Tough New Law against Coronoavirus: Why it's Disquieting," *The Conversation*, April 7, 2020, *available at* <https://theconversation.com/ghanas-president-has-invoked-a-tough-new-law-against-coronavirus-why-its-disquieting-135476> (last visited Nov. 28, 2022); K. Appiagyei-Atua, "Emergency without a State of Emergency: Effect of Imposition of Restrictions Act, 2020 on the rights of Ghanaians," My Joy Online, April 2, 2020, *available at* <https://www.myjoyonline.com/emergency-without-a-state-of-emergency-effect-of-imposition-of-restrictions-act-2020-on-rights-of-ghanaians/> (last visited Nov. 28, 2022); K. Agyeman-Budu, "COVID-19, Constitutionalism and Emergencies under Ghana's 1992 Fourth Republican Constitution," Verfassungsblog, May 23, 2020, *available at* <https://verfassungsblog.de/covid-19-constitutionalism-and-emergencies-under-ghanas-1992-fourth-republican-constitution/> (last visited Nov. 28, 2022).
77. M. M. Mello and C. J. Wang, "Ethics and Governance for Digital Disease Surveillance," *Science* 368, no. 6494 (2020): 951-954.

The Journal of Law, Medicine & Ethics, 50 (2022): 791-804. © 2023 The Author(s)