IDC HERZLIYA | Lauder School of Government, Diplomacy & Strategy | Program on Democratic Resilience & Development

Konrad Adenauer Stiftung

Digital Contact Tracing Has Failed: Can it be Fixed with Better Legal Design?

Elad D. Gil

Working Paper

2/2021

February 2021

Digital Contact Tracing Has Failed: Can it be Fixed with Better Legal Design?

Elad D. Gil[*]

2/2021

February 2021

[*] Post-Doctoral Fellow, Hebrew University, Faculty of Law and the Federmann Cyber Security Center; Research Fellow, the Abba Eban Institute for international Diplomacy, the Interdisciplinary Center Herzliya.

Abstract

Can big data-driven technology help contain the spread of infectious diseases? Based on the Covid-19 experience, the answer seems to be 'no'. Despite a global-wide effort by governments, developers, and research institutions to harness technology to the fight against coronavirus, digital contact tracing has failed almost everywhere. But a closer analysis, informed by comparative data, reveals that this failure was not inevitable. The crisis required local and national governments to evaluate the societal harms and benefits of the technology in conditions of uncertainty, but the legal frameworks governing that effort were ill-suited for health emergencies. And thus, a series of factors that originated from or grew bigger by overhyped anxiety over the erosion of the right to privacy prevented the technology from living up to its potential. This essay argues that better legal and institutional design can facilitate a more rational and efficient process for dealing with privacy versus public health tradeoffs in times of pandemics. It then sketches the essential features of a new framework health emergency law and explains its advantages over the classic legal frameworks applied by most democratic states during emergencies.

CONTENTS

1. INTRODUCTION: DIGITAL CONTACT TRACING GOES GLOBAL AND FAILS

On March 11, 2020, the World Health Organization (WHO) declared COVID-19 a pandemic, noting that "there are now more than 118,000 cases in 114 countries, and 4,291 people have lost their lives."[1] As of this writing, on January 19, 2021, there are more than 93 million confirmed cases, including 2.03 million deaths globally.[2] Over 500,000 new cases were confirmed yesterday;[3] and many countries are in the midst of a second wave or the beginning of what appears to be a third wave of the outbreak.[4] The numbers make clear that the effort to control or contain the spread of the virus has failed. Experts generally agree that much of the blame rests on the poor performance of contact tracing—the process of interrupting community transmissions, by identifying and isolating persons who have been in close proximity to confirmed patients.[5] Contact tracing is an established technique for containing diseases, traditionally performed 'manually' by health officials who interview confirmed patients to track their contacts. But the exponential nature of COVID-19 infections and the high incidence of asymptomatic carriers have rendered traditional tracing practices largely ineffective as a tool for suppressing community transmissions.

Early in the pandemic, as the SARS-CoV-2 virus began to spread across the world, many governments turned to data-driven technologies for answers. One prominent area in which technology was thought to make a critical contribution was contact tracing.[6]

---

[1] World Health Organization, WHO Director-General's opening remarks at the media briefing on COVID-19 (Mar. 11, 2020). https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[2] WHO Coronavirus Disease (COVID-19) Dashboard (Data last updated: Jan. 19, 2021, 9:49AM CET) https://covid19.who.int/?gclid=CjwKCAiArIH_BRB2EiwALfbH1Kc9eEMk_-nO7P1xjsL0ceB8Gl29RQh7pL24L_ZJfOdMTeTCQtLkVhoCFIwQAvD_BwE

[3] Id.

[4] See Barigazzi J. (2020) 'WHO COVID envoy warns of third wave in Europe in 2021', *Politico*, 22 Nov. https://www.politico.eu/article/coronavirus-third-wave-europe-2021-world-health-organization-envoy/

[5] Researchers have shown that contact tracing can be an effective measure if carried early in the life cycle of epidemics. See Ferretti L. et al. (2020) 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', *Science* 368; Kretzschmar M. et al. (2020) 'Isolation and Contact Tracing Can Tip the Scale to Containment of COVID-19 In Populations with Social Distancing', 23 Mar. Available at SSRN: https://ssrn.com/abstract=3562458. It is widely agreed that many countries, including the U.S. and European countries, were late in developing functioning contact tracing apparatuses and that it is poorly managed. See, e.g., Lewis D (2020) 'Where COVID Contact Tracing Went wrong', *Nature* 588 384-388 (Dec. 2020); Barry E & DePasquale R. (2020) 'Officials scale back contact tracing efforts in the U.S., saying they cannot keep up', *N.Y. Times Corona Virus Live Update*, 30 Nov. https://www.nytimes.com/live/2020/11/24/world/covid-19-coronavirus#officials-scale-back-contact-tracing-efforts-in-the-us-saying-they-cannot-keep-up.

[6] Benjamin G. C. (2020) 'The Secret Weapon Against Pandemics', *TED2020*, 20 May. https://www.ted.com/talks/georges_c_benjamin_the_secret_weapon_against_pandemics/transcript. See

Governments, research institutions, and for-profit corporations—including Apple and Google, two of the world's major technology companies—led, participated, funded, and collaborated in efforts to automate contact tracing ("digital contact tracing," or "DCT") and help build a tracing apparatus that would dramatically outperform the traditional process in scale, efficiency, and speed. It was believed that DCT would allow communities to avoid or limit the need for lockdowns and other restrictions on movement, enabling rapid societal and economic recovery without risking epidemiological catastrophe.[7]

As late as April 2020, the first technology-enabled contact tracing measures were introduced in Southeast Asia and Israel.[8] Apple and Google rolled out their exposure notification interface in May.[9] Since then, many developers and government agencies across the world have launched an array of DCT tools.[10] But after nine months, the vast majority of these measures have not made much of a difference in most of the world. Particularly in the West, contact tracing fell far short of meeting the WHO benchmark of 80% tracing within three days.[11] Data collected from over 50 countries show that there is no one factor that accounts for the poor record of digital contact tracing.[12] It failed in countries that allowed it to operate only under the most stringent privacy restrictions, as well as in countries that sanctioned intrusive nationwide surveillance regimes, such as Israel.[13] It struggled in countries that adopted voluntary, opt-in apps, as well as in countries that enforced mandatory participation. Finally, it was inaccurate and of limited use regardless of its *technology* (Bluetooth vs. location-enabled), *architecture*

---

also Park A. (2020) 'The Tech That Could Be Our Best Hope for Fighting COVID-19—and Future Outbreaks', *Time*, 19 Mar., https://time.com/5805622/coronavirus-pandemic-technology/.

[7] Moreover, efficient contact tracing provides valuable data for researchers on where and in what circumstances infections occurred most frequently. These data, in turn, can help policymakers develop optimal exit strategies from lockdowns and ease restrictions in places where infections are less likely.

[8] Kharpal A. (2020) 'Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends', *CNBC*, 30 Mar. https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html.

[9] Schumaker E. (2020) 'Apple and Google launch digital contact tracing system, *ABC News*, 6 May. https://abcnews.go.com/Technology/apple-google-launch-digital-contact-tracing-system/story?id=70789376

[10] For a survey of measures implemented in U.S. states and around the world see Kissick C. et al. (2020) 'What Ever Happened to Digital Contact Tracing?' *Lawfare*, 21 Jul. https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing.

[11] The failure, to be sure, is not only technological. Efforts to test and track infections have been understaffed; testing has been slow, those infected frequently did not cooperate with epidemiological investigations, and people who have been found to be in close contacts with infected persons were reluctant to self-quarantine themselves. But even with the other factors present, it is evident that technology has not delivered on its promise to turn contact tracing into a wide scale, faster, smarter, and effective process.

[12] See MIT Covid Tracing Tracker data base, https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx_zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit#gid=0 (last visited 14 Jan. 2021) (hereinafter, MIT Covid Tracing Tracker).

[13] For analysis of the Israeli tracing model in comparative perspective, see Shwartz Altshuler T. & Aridor Hershkovitz R. (2020) 'Coronavirus: Israeli and Comparative Perspectives', *Brookings Inst*.

(centralized vs. decentralized) or *implementation method* (top-down vs. bottom-up). No one of these factors by itself accounts for the failure.

In the democratic world, a combination of three factors accounted for the failure of digital contact tracing: low usage rates, technical hurdles, and technological 'tyranny' of the private sector.[14] In order to fix digital contact tracing, each of these factors must be addressed. Interestingly, all three stem from the same root cause- a reflexive sentiment across democratic societies to protect privacy at (what in hindsight can plausibly be viewed as) unreasonable costs. Especially in the West, a well-earned loss of trust in both the government and the tech industry triggered an uncompromising, perhaps irrational commitment to privacy and control of personal data, while other fundamental rights and public interests were easily surrendered.[15] The first step in unlocking the potential of digital contact tracing is to create the legal conditions for a more rational process to deal with privacy versus public health tradeoffs. This essay argues that to establish the conditions for technology to be more effective, we need better law for managing health emergencies—a legal framework that enters into force when pandemics erupt and sunsets when they wane. Currently, in most countries, the legal response to the outbreak relies on one of two legal models for managing emergencies:[16] The first is a continuation of the normal constitutional order, known in the literature as the 'business as usual' model.[17] Under this model, the government must act on the basis of legislation and its ability to limit the exercise of constitutional rights is strictly confined.[18] The second approach is invoking an emergency clause in the constitution that entrusts the executive with broad powers and relaxes or suspends the normal system of checks and balances.[19] Neither approach, I argue, is appropriate for the circumstances arising in a pandemic. Health crises are a special species of emergency. Better design of the legal frameworks governing public health emergencies could accommodate a more effective DCT policy, without disproportionate risks to human rights.

The remainder of this essay develops this argument. Part II explores the three main reasons underlying the failure of DCT across the world and shows how each of them

[14] See infra Part II.

[15] See Bambauer J. & Ray B. (2020) 'Covid-19 Apps are Terrible—They Didn't Have to be,' *The Digital Social Contract: A Lawfare Paper Series*.

[16] See Ginsburg T. & Versteeg M (2020) 'The Bound Executive: Emergency Powers During the Pandemic' (Jul. 26, 2020) Virginia Public Law and Legal Theory Research Paper No. 2020-52, U of Chicago, Public Law Working Paper No. 747, Available at SSRN: https://ssrn.com/abstract=3608974.

[17] See Gross O. (2003) 'Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?' Yale L.J. 112, 1011:1134, 1043:58. Some scholars refer to this model as the "legislative model". See Ferejohn J. & Pasquino P. (2004) 'The Law of the Exception: A Typology of Emergency Powers', Intl J. Con. L. 2, 210:239.

[18] Id., at 215.

[19] As employed in democratic states, the emergency model has also been described as "constitutional dictatorship," modeled on the Roman system of emergency powers. See Rossiter C. (1948) *Constitutional Dictatorship: Crisis Government in the Modern Democracies* Princeton.

originated or expanded from a deeply rooted but overhyped anxiety over the erosion of the right to privacy. Part III makes the case for creating a special legal framework for pandemics and lays out its central substantive and procedural components. This discussion focuses on digital contact tracing and does not consider other aspects of health-emergency governance; however, its insights can also inform broader debates about pandemics law. A short conclusion follows.

The aim of this essay is not merely to delve into the failures of the COVID-19 crisis. Even with vaccines in sight and the prospect of some relief, new and more contagious variants of COVID-19, discovered in the U.K. and South Africa, and the possibility of future pandemics, may give rise to far worse health crises, and requiring an energetic and focused effort to save human lives and prevent economic disaster. The conversation about the proper legal framework to govern pandemics should begin now, rather than waiting for the next phase of the current crisis or a new crisis.

2. WHAT WENT WRONG?

This section describes why, in most countries, technology-enabled contact tracing has been marginalized, if not abandoned. It identifies three main reasons: low usage rates, technical failures, and private sector technological dominance.

2.1. LOW USAGE RATES

A precondition for effective contact tracing is that as many contacts as possible are identified and isolated before they infect another person. Researchers at Oxford University have developed a model which suggests that around 56% of the total population has to be tracked, in order to stop an outbreak, although even lower usage rates may help slow down the spread of the virus.[20] The main challenge in meeting or coming close to this threshold is that participation is voluntary in almost all parts of the democratic world. People must give their consent, downloading a smartphone app or use another device provided to them, and self-quarantine, upon receiving notification of exposure.[21] In most cases, it is also up to the infected person to voluntarily alert other

[20] Hinch R. et al. (2020) 'Effective Configurations of a Digital Contact Tracing App: A report to NHSX', at *9, 16 Apr.

[21] All apps and systems used within the U.S., both state and privately managed are voluntary. See Hecht-Felella L. & Mueller-Hsia K. (2020) 'Rating the Privacy Protections of State Covid-19 Tracking Apps,' *Brenan Ctr. for Justice* (Nov. 5, 2020) https://www.brennancenter.org/our-work/research-reports/rating-privacy-protections-state-covid-19-tracking-apps. Outside the U.S., some countries require participation in specific circumstances, but for the most part participation is not legally required. See Law Library of

users, by sharing a code that sends an in-app anonymized message.[22] This means that the authorities must convince people that signing on is safe and beneficial for them. Surveys conducted at the early stages of the pandemic suggested that reaching the desired usage rates is feasible, with around 80% of participants saying that they would definitely or probably install state-backed apps in their phones.[23]

In reality, however, convincing people to embrace the technology has proved challenging. Only a handful of countries have come close to the desired uptake levels, and the average is below 20%.[24] Within the U.S., penetration rates are even lower. As of early December, around 20% of the population in Colorado, Connecticut, and Maryland have been using that state's official app, while usage in Washington has been 13%, with the rest of the states that launched an official app below 10%.[25] Rates have recently increased, with the release of the new version of the Apple-Google system that does not require a third-party app; however, participation rates in most states they are still relatively low.[26]

From the outset, privacy concerns and distrust of the government and technology companies have been major barriers for wide public adoption of the apps. Since the attacks on 9/11, and especially in the last decade, revelations about the breadth and scope of government surveillance have drawn greater public attention to the risks to privacy and liberty in the digital age.[27] People have discovered that, without their knowledge or consent, their personal information was intercepted and collected by government agencies. On occasion, decisions affecting individual liberty were made based on this personal data. Many feared, rightfully so, that the 'privacy vs security' framing that dominated public discourse in the wake of 9/11 and used to excuse unchecked surveillance powers will resurface as a 'privacy vs health' argument for the very same purpose. The skepticism surrounding government access to private information was compounded by discomfort over pervasive corporate surveillance.[28]

Congress (2020) 'Regulating Electronic Means to Fight the Spread of COVID-19,' at 2 (hereinafter, Library of Congress Rep.).

[22] See, e.g., Covid Watch: Arizona Exposure Notification App https://covid19.arizona.edu/covidwatch (last visited December 22, 2020).

[23] See Milsom L. et al., Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy (Jul. 2020) https://osf.io/7vgq9/.

[24] This includes Finland, Iceland, and Singapore, whose penetration rates range between 38-49%. Below them are 12 countries with penetration rates of 10-30%, and the rest are in single digits. MIT Covid Tracing Tracker, supra note 12.

[25] Valentino-DeVries J. (2020) 'Coronavirus Apps Show Promise but Prove a Tough Sell,' *N.Y. Times* Dec. 7. https://www.nytimes.com/2020/12/07/technology/coronavirus-exposure-alert-apps.html.

[26] De la Garza A. (2020) 'People Are Finally Downloading COVID-19 Exposure Notification Apps. Will They Make a Difference?,' *Time,* Dec. 14. https://time.com/5921518/covid-exposure-notification-apps/.

[27] For an overview of the U.S. surveillance policies see, e.g., The President's Review Grp. on Intelligence and Commc'ns Techs., Liberty and Security in a Changing World (2013).

[28] See Zuboff S. (2019) *The Age of Surveillance Capitalism*, Profile.

Affairs such as the Facebook-Cambridge Analytica scandal and the Equifax data breach have brought to light the dangers of inadequate data security and the numerous ways by which private firms collect, analyze, share, and sell personal data, without the knowledge or consent of users.

This not unfounded fear over the loss of privacy and accumulation of personal data by governments and companies provoked legal and societal backlash. New laws and institutions were created across Europe and in the U.S. to safeguard privacy and ensure the proper handling of personal data. Privacy became a concern that engineers had to take seriously in developing new products, an approach known as "privacy by design." When the pandemic erupted in the winter of 2020, it encountered societies traumatized by a sense of constant surveillance, as well as national and regional legal regimes specifically designed to constrain efforts by governments or private companies to further erode people's privacy.[29]

From the beginning, therefore, public discourse about digital contact tracing revolved around privacy and involved institutional actors whose mandate was to protect it.[30] This framing had two major implications. First, before the conversation even started, it nurtured a political climate in which some ideas were taken off the table, even though they might have had clear advantages from a public-health perspective. For instance, insofar as the success of DCT depends first and foremost on usage rates—and that success means fewer restrictions on the liberty to move, work and socialize, then why not at least consider the use of legal sticks and carrots to encourage participation? But that was hardly the case. In Europe, for example, the EU Data Protection Board (EDPB) issued guidelines that monitoring locations or contacts between persons "can only be legitimised by relying on a voluntary adoption by the users."[31] And the Apple and Google platform, on which many states apps operate, is premised on voluntary adoption and information sharing and bans collection of location information, even with users approval.[32] Second, the focus on privacy affected product design choices in ways that apriori maximized privacy at the expense of efficiency. As one study put it, "the

[29] For example, one survey showed that only 26% of participants believed that data collected by the government for COVID -19 mitigation would be used only for that purpose. Moreover, 60% expressed concerns that government data collection would adversely affect their safety or the safety of others. See Simko L. et al. (2020) 'COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences,' *U. Wash. Security Lab Covid-19 Relate Res.* (Rep. Ver. 1.0) 8 May.

[30] To illustrate, civil society organizations and research institutes analyze and rank apps, based mostly on their privacy and data security features, but show much less interest in their efficacy. See, Brenan Ctr. Covid Apps privacy ranking, supra note 21; MIT Covid Tracing Tracker, supra note 12.

[31] E.U. Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (Apr. 21, 2020) (hereinafter, EDPB Guidelines), at 7.

[32] See Apple & Google, Exposure Notifications (2020) 'Frequently Asked Questions v. 1.2'. https://static.googleusercontent.com/media/www.google.com/iw//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf

reluctance to leverage communications technologies to stem the spread of the novel coronavirus was so strong and so pervasive that the COVID-19 apps in operation today are underpowered and undersubscribed by design."[33] Nearly all of the apps created for DCT in the U.S. and Europe were geared to maximize user privacy and ensure that access to sensitive information is strictly limited.[34] Even then, privacy advocates were still critical and suspicious.[35] In some places, the anxiety over privacy was so embedded in the political discourse that legislatures blocked state agencies from adopting even the most privacy-preserving technologies.[36]

Compromising on voluntary, opt-in-based tracing regimes and privacy-maximizing product designs was believed by decisionmakers to boost public confidence in the technology. The rationale was that apps would be somewhat less effective but would attract more people to sign on; the net effect would be privacy-preserving yet widely adopted digital contact tracing programs.[37] However, as the current penetration rates show, the focus on privacy did not yield high acceptance rates. It merely left with suboptimal products, as follows.

2.2. TECHNICAL HURDLES

Another major barrier to effective digital contact tracing stems from technical limitations. None of the technologies used today for digital contact tracing, including Bluetooth, GPS, tower data from mobile phone, and other technological applications that leave digital footprints, was designed for contact tracing. While these technologies produce data that

[33] Bambauer & Ray, supra note 15.

[34] In the U.S., for example, 20 out of 23 states use the decentralized, proximity-based Apple-Google interface exclusively. Only Wyoming, North Dakota, and South Dakota enable centralized data collection, which runs on a voluntary, opt-in participation. See Brenan Ctr., supra note 21 (data is updated to Nov. 5, 2020).

[35] See, Calo R. (2020) 'Enlisting Big Data in the Fight Against Coronavirus, written testimony before the Senate Committee on Commerce, Science, and Transportation, at 3, 9 Apr. https://www.commerce.senate.gov/services/files/D069F0C0-2B67-4999-AC75-5BC41D14D00C; Long C. (2020) *Privacy and Pandemics, in Law in the Time of Covid-19* (Pistor K. ed.) [online] ("The slope from non-anonymized COVID-19 immunity databases, to governmental collection of non-anonymized information about individuals' immunity status to other viruses, then to their vaccination records, then to their public health wellness generally, is a slippery one indeed").

[36] For example, lawmakers in South Carolina blocked state agencies from implementing contact tracing apps using the Apple and Google platform. See Perera D. (2020) 'South Carolina legislature puts coronavirus apps on hold,' M.Lex, 26 Jun. https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-carolina-legislature-puts-coronavirus-apps-on-hold

[37] See Albergotti R. & Harwell D. (2020) 'Apple and Google are building a virus-tracking system. Health officials say it will be practically useless,' Wash. Post, 15 May. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/ (reporting that according to Apple and Google "limiting the data the apps use could bolster their adoption rate, because people may not trust or use an app that logs their location for later use by public health authorities").

can be helpful for this application (and for this reason, attracted so much attention from governments and developers), using any of them will be effective in only some cases. Any technological measure adopted will result in some rate of false positives—cases in which a person is incorrectly identified to have come into contact with a carrier, and false negatives—cases in which a close contact with a carrier is not identified by the system. The practical implication of frequent errors is that people who are notified of an exposure by a system they cannot trust may not be willing to self-quarantine, and that people who are not notified may nonetheless have been exposed, rendering the value of the app minimal. Over-trust in the apps, also a possibility, can lead to excessive and unnecessary self-restriction in some cases and a false sense of safety that may increase infections in others.[38] In other words, if the technology is not accurate enough, its public health benefits could be outweighed by its costs. Moreover, if people are confused or frustrated using the technology, all efforts to encourage wide adoption in the community are doomed to fail.

Now and for the foreseeable future, no one technology can significantly eliminate or reduce the risks of erroneous notifications and non-notifications.[39] Location-based products are not accurate enough for contact tracing. While the Centers for Disease Control (CDC) defines 'close contact' as "any individual within 6 feet (i.e., roughly 2 meters) of an infected person for a total of 15 minutes or more,"[40] the resolution of GPS in a smartphone is 16-41 feet at best and depends on many variables, including physical location, satellite geometry, signal blockage, and atmospheric conditions.[41] Other sources used to detect location, like triangulation from nearby cell towers and Wifi signals, are even less accurate and reliable.[42] Bluetooth-based proximity detection offers some advantages in terms of precision but has its own shortcomings. Bluetooth makes inferences of distance between two devices based on the strength of signal, yet the signal is affected not only by distance but by many other factors, such as the phone's receiver, operating system configuration, antenna layout, hardware, and reflections from physical surroundings.[43] The resulting fluctuations can cause Bluetooth-enabled apps to

[38] See Gray S. (2020) 'Enlisting Big Data in the Fight Against Coronavirus, written testimony before the Senate Committee on Commerce, Science, and Transportation,' at 35-36, 15 Apr.

[39] See, Schneier B., Me on COVID-19 Contact Tracing Apps,' *Schneier on Security*, 1 May. https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html.

[40] CDC, Contact Tracing for COVID-19, https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/contact-tracing.html (last visited, Dec. 29, 2020).

[41] See Robinson A. & Waldo J. (2020) 'Technical Difficulties of Contact Tracing,' *Lawfare*, 17 Dec. https://www.lawfareblog.com/technical-difficulties-contact-tracing; National Coordination Office for Space-Based Positioning, Navigation, and Timing, GPS Accuracy, https://www.gps.gov/systems/gps/performance/accuracy/ (last visited, 29 Dec. 2020).

[42] Stanley J. & Granick J. (2020) 'The Limits of Location Tracking in an Epidemic, *ACLU*, at 3-4, 8 Apr. https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf

[43] See Robinson & Waldo, supra note 41; Leith D. J. & Farrell S. (2020) 'Coronavirus Contact Tracing: Evaluating the Potential of Using Bluetooth Received Signal Strength for Proximity Detection,' *ACM SIGCOMM Computer Communication Rev.* 50.

register false exposures (inferring that devices are closer than they are in reality) in some conditions and not to identify real exposures in others.

Reducing the rates of false positives and false negatives is technologically feasible. South Korea's tracing system was highly effective, because it integrated several data sources, including GPS location data, credit card transactions, closed-circuit television footage, and records of government services s.[44] In a recent study employing similar logic, a team of researchers from MIT argued that the key to improving digital contact tracing is pairing proximity-based tracing with what they call "global context," namely, location and time data.[45] Because each technology has different limitations, using both Bluetooth and location data eliminates some of the uncertainties and errors. Currently, the Apple-Google Exposure Notification System delivers information to users and public health authorities that has only limited context: an exposure notification allows users to know the day of exposure, its duration, and the strength of signal (that indicates the level of proximity, to some degree).[46] Providing more granular context—for example, by analyzing location data or other context factors—would allow users to modify their behavior and better assess the risk of exposure (e.g., they left their device at the office, or were outdoors wearing a mask). For the authorities, learning about locations and times of exposure provides valuable information about places and times in which the risk of exposure is high. Overall, better context can help the authorities in optimizing contact tracing efforts (e.g., first calling people who were exposed indoors for longer periods of time). But while using a combination of Bluetooth and location data is promising, it raises privacy issues and does not comply with the Apple-Google specification, which does not allow apps using its system to keep location logs.[47] Indeed, the MIT study strains to include features that produce global context within Apple-Google's strict privacy limitations.

It follows that making digital contact tracing more efficient is feasible but involves privacy and data security tradeoffs. Are these tradeoffs inevitable? Should this path nonetheless be followed? Part III will consider these questions. But before this discussion can start, one more drawback to DCT should be addressed, the tyranny of the tech industry.

[44] See Park S. et al. (2020) 'Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies', *J. Am. Med. Association* 323 2129:2130.

[45] Raskar R. et al. (2020) 'Adding Location and Global context to the Google/Apple Exposure Notification Bluetooth API,' Eprint arXiv:2007.02317 [cs.CR], 25 Jul. https://arxiv.org/abs/2007.02317

[46] Apple & Google, Exposure Notifications: Frequently Asked Questions, at 5-6 (Sep. 2020) https://static.googleusercontent.com/media/www.google.com/iw//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf

[47] Id.

2.3. PRIVATE SECTOR TECHNOLOGICAL DOMINANCE

During the coronavirus pandemic, government power was constrained by a new type of force—one that classic state of emergency literature does not account for: the tech industry, particularly the tech giants, Apple and Google. In this crisis, these actors claimed a seat at the table, and then utilized their powerful position to impose what they saw as the 'correct' balance between privacy and public health. Their dominance hindered the introduction of DCT measures around the world, caused national and state governments to suspend or scratch their preferred technologies, rendered incompatible apps inefficient, and sought to dictate strict privacy standards for the whole world.

In April, when governments and private firms were working to develop their versions of contact tracing apps, Apple and Google announced their joint venture. The application programming interface (API) they built, which initially let developers design the apps, overcame a major technological obstacle for customized contact tracing apps that rely on Bluetooth technology. Especially on Apple devices, apps running in the background were not allowed to access Bluetooth and obtain new contacts. To perform this essential function, the user was required to keep the phone unlocked, with the app running in the foreground, at a cost in battery life and significant inconvenience. The newly developed API resolved this issue but imposed strict rules for developers. Apps designed for the new interface are not allowed to collect location data; their communication protocol must be decentralized; they must receive user consent for operating and separate consent for sharing the data with public health authorities; and data collected are subject to strict minimization rules.[48]

The new API put a halt to systems that did not adhere to these architectural rules.[49] Some states, like the U.K., Norway, and Germany, ultimately decided to accept Apple and Google's dictates and abandoned the tracing models they initially found most useful.[50] Especially in the U.K., the shift caused major setbacks in the launch of new apps.[51] Other countries, including France, Israel, Australia, and New Zealand, insisted on moving forward with their original systems, admitting that they would not function optimally on Apple and Google devices. France and Germany initially asked Apple to relax some of the iPhone privacy features that diminish the functionality of their desired

[48] See O'Neill P. H. (2020) 'Google and Apple ban location tracking in their contact tracing apps', *MIT Tech. Rev.*, 4 May. https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/

[49] See Scott M. et al. (2020) 'How Google and Apple outflanked Governments in the Race to Build Coronavirus Apps', *Politico* (May 15, 2020, 5:25 AM) https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/.

[50] See Shead S. (2020) 'In Major U-turn, the UK will now use Apple and Google's Platform for its Coronavirus Tracing App', *CNBC*, 18 Jun. https://www.cnbc.com/2020/06/18/apple-and-googles-tech-to-underpin-uk-contact-tracing-app.html.

[51] See Cellan-Jones R. (2020) 'Coronavirus: What went wrong with the UK's contact tracing app?', *BBC News*, 20 Jun. https://www.bbc.com/news/technology-53114251.

apps, but the company did not bend.[52] And there was no legal means for these governments to force the companies to change their positions. As one commentator put it, "in the digital fight against Covid-19, Big Tech squared off against governments — and won."[53]

The irony, according to some experts, is that while the two companies jealously prohibit anything beyond minimal and, arguably, suboptimal data collection to slow down a global life-threatening pandemic, they continue collecting and processing users personal and location data on a massive scale, for their own commercial needs.[54] For nearly two decades, the companies have also complied with U.S. laws that require them to produce sensitive personal data to the government upon request.[55] Why the sudden effort to recast themselves as champions of privacy? The answer lies in the bigger picture. This recent effort did not originate with the COVID-19 crisis but dates back to the backlash following the Snowden revelations, in which their part in U.S. surveillance programs became public. This effort serves a deliberate strategy on their part to respond to the growing awareness—and anxiety—among their worldwide users over digital surveillance and other societal harms caused by their products. There is nothing illegitimate with private companies aiming to keep their customers and stakeholders satisfied. But when private actors, driven first and foremost by their own economic interests, dictate the response to a global pandemic, alarm bells should go off. As one scholar notes, the concern is that "the (legitimate) advantage that tech companies have accrued in the sphere of the production of digital goods provides them with (illegitimate) access to the spheres of health and medicine, and more worrisome, to the sphere of politics."[56]

To be sure, there are positives in Apple and Google's role in placing boundaries on how states wield power in this domain.[57] Digital surveillance is prone to government abuse. Fears that personal data collected for disease surveillance will be used for ill or breached by rogue actors are not unfounded. Recent reports suggest that data concerning approximately 32,000 people, mainly Israelis, was leaked from a contact tracing system developed by NSO Group, an Israeli cyber firm.[58] Early in the pandemic, several countries adopted overly intrusive tools that have not proved effective in slowing down the epidemic. In contrast, Apple and Google's API demonstrated greater concern for

[52] Scott, supra note 49.

[53] Id.

[54] See Bambauer & Brian Ray, supra note 15, at 19; Albergotti & Harwell, supra note 37.

[55] See, e.g., FISA, 50 U.S.C. § 1805; FISA Amendments Act § 702, 50 U.S.C. § 1881a.

[56] Sharon T. (2020) 'Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers,' Ethics and Info. Tech. 2020, 1:13.

[57] Cf., Rozenshtein A. Z. (2018) 'Surveillance Intermediaries,' Stan. L. Rev. 70 99:189.

[58] See, NSO Group's Breach of Private Data with 'Fleming,' a Covid-19 Contact Tracing Software, Forensic Architecture (31 Dec. 2020) https://forensic-architecture.org/investigation/nso-groups-breach-of-private-data-with-fleming-a-covid-19-contact-tracing-software (reporting that a database of more than five hundred thousand datapoints for more than thirty thousand distinct mobile phones uploaded to the Fleming demo remained unprotected).

individual rights and made a genuine effort to develop an exposure tracing system which preserved privacy. In September, when it turned out that many customized apps running on the new API were off to a rocky start, the two companies launched a new version of their system that does not require a third-party app and makes it easier for the authorities to deploy.[59] We should be worried, however, when, in times of crisis, the ability of governments to deliver an essential public good is constrained by corporate actors. Notwithstanding their contributions to the fight against COVID-19, the transparency and accountability of these companies are minimal at best. Given that there is no one 'correct' balance between public health and other rights and interests at play in the design and implementation of digital contact tracing tools, the balance should be subject to democratic political processes and constitutionalism, not corporate interests.

3. RETHINKING THE LEGAL FRAMEWORK GOVERNING HEALTH CRISES

3.1. WHY THE CLASSICAL MODELS OF EMERGENCY GOVERNANCE ARE INAPPROPRIATE

Against the backdrop of the outbreak of the novel coronavirus, the first generation of contact tracing apps was launched by trial and error. It still may be too soon to tell whether the technology is fully developed and can, in any configuration, meaningfully reduce the rate of transmission. But given the dire outcomes so far, the recently discovered, more contagious variants, and the relative success of DCT in places such as South Korea, an effort to make the technology more effective is at least an option worth investigating. Effective contact tracing could reduce the death toll and economic loss, limit restrictions on the freedoms of movement, assembly, and worship, and ease other types of mental, economic, and physical hardship caused by recurring lockdowns. Based on the foregoing, in order to be successful, digital contact tracing requires: (1) significant usage rates, which require, at the very least, some restrictions on people who do not sign on;[60] (2) the capacity to collect, process, and share with health authorities data from several sources, including location data; and (3) to be subject to *democratic* governance—that is, unconstrained by the dictates of the tech sector, yet relying on private-public collaboration and mutual trust.

[59] Google, Exposure Notifications Express overview (11 Sep. 2020) https://developers.google.com/android/exposure-notifications/en-express. Notably, the new interface gives health authorities control of the risk parameters for triggering an exposure notification. That essentially means that they have a choice between configurations that risk more false positives or false negatives.

[60] This assertion is based on the current adoption rate statistics. As noted, no country that runs voluntary apps had reached a 50% adoption rate mark. The global average is around 20%. See MIT Covid Tracing Tracker, supra note 12.

Could these conditions be met, without limiting privacy, autonomy, and data security? Probably not. Is limiting these rights to enable effective digital contact tracing desirable from a social welfare perspective? The answer depends on the subjective value one attaches to the social harms and benefits involved (privacy, autonomy, liberty, life, economic harms, mental harms, etc.), and probably varies with the circumstances (the more lethal a pandemic, the more people would agree to limit rights). But before weighing the competing rights and interests, decision-makers should try to minimize the degree to which rights are limited to enable effective DCT, and only then to debate the remaining tradeoffs.[61] Put another way, policymaking which implicates the limitation of rights should follow two steps: the first is an effort to minimize risks to the rights implicated in order to make policy more efficient; the second is an effort to strike the right balance between the competing rights and interests.

The legal and public debates on digital contact tracing did not involve, at least- did not exhaust, the first step, and failed accurately to carry out the second step. One reason, mentioned above, is the disproportionate attention given to privacy over other values.[62] Not unrelated to the first, is another reason: ill-suited legal frameworks. In the context of pandemics, neither of the two classical models of crisis governance provides the necessary conditions for dealing with appropriate tradeoffs.

Under the *business-as-usual model*, the ordinary system of checks and balances remains in place during the crisis, and constitutional and, where applicable, supra-constitutional, protections of rights continue to apply with equal or almost equal force.[63] This constitutional architecture has two implications in the current situation: first, it legally limits the degree to which policies can contemplate measures infringing on privacy and liberty, such as movement tracking and opt-out or mandatory participation.[64] While the protection of rights is always contextual and allows some tradeoffs, the discretion given to health authorities is limited and non-deferential. This was evident in the case of the

[61] The assertion that minimization of social costs precedes the process of balancing is inherent in the principle of proportionality, a leading frame for considering conflicts over constitutional rights in many legal systems. See Barak A. (2012) *Proportionality: Constitutional Rights and their Limitations*, Cambridge. The idea is also featured in frameworks adopted by U.S. scholars with respect to national security emergencies. See Posner A. & Vermeule A. (2007) Terror in the Balance: Security, Liberty, and the Courts, 21-24 Oxford. For a useful analysis of Posner & Vermeule's thesis from this perspective see Rozenshtein, supra note 57, at 163-65.

[62] See supra, at Part II.A. See also Bambauer J. et al. (2020) 'It's Time to Get Real About COVID Apps, Fighting Covid with Data working grp., 14 May. https://medium.com/@DataVersusCovid/its-time-to-get-real-about-covid-apps-dd82e08895f2

[63] Countries that have followed this model during the COVID -19 crisis include the U.S., Germany, France, Australia, Poland, Belgium, Japan, and South Korea, among others.

[64] For example, national contact tracing apps can work across EU borders only if they comply with a set of technical specifications agreed to by the E.U. Commission, which include voluntary adoption, no requirement for geolocation tracking, and sufficient data protection and privacy guarantees. See Commission Implementing Decision 2020 (EU) 2020/1023 15 Jul.

Norwegian app, which traced movements and recorded locations on a centralized server.[65] In August, the Norwegian Data Protection Authority banned the app, overruling the position of the country's Institute of Public Health, after it was found to impose disproportionate "intervention in the users' fundamental rights to data protection."[66] Second, this architecture fails to contemplate special safeguards that are typically built in emergency regimes, to balance broader authority and tighter oversight. If f business is as usual, there is no need for special safeguards. Accordingly, the assumption of business-as-usual limits the effort of minimization.

Moreover, because the normal legal order remains in force, there is greater concern that exceptional measures could have long-term effects on civil rights and might normalize state surveillance. Finally, at the sociological level, the business-as-usual model fails to convey to the public and the business sector that the crisis is serious enough to merit some tradeoffs to better protect public health, and so less cooperation is more likely.

The competing model of *special emergency powers* raises other problems. In response to emergency situations, many constitutions permit the suspension of the normal legal order.[67] The rationale is that, in times of grave risk to the state or its population, the legal system should accommodate the most pressing public interest at the moment—averting the emergency, even at the expense of other important social and constitutionally significant values. A typical state of emergency regime temporarily shifts powers normally allocated between the branches of government (and local governments, where applicable) to the national executive and permits greater limitations on civil liberties insofar as necessary to deal with the crisis.[68] While it may appear that the emergency model is a better fit for a DCT regime based on the above criteria, this is not the case. The major problem with this approach, which treats all types of emergencies the same way, is that many of its premises and, consequently, the tools it prescribes, are not relevant in health emergencies. In pandemics, there is no enemy from which it is crucial to conceal the government's aims and plans. Unlike national security-driven surveillance, disease surveillance need not be kept secret to work.[69] The information required for

[65] See E.U. Data Protection Board, Temporary suspension of the Norwegian Covid-19 contact tracing app, EUDPB National News (22 Jun. 2020) https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en

[66] Id.

[67] Ginsburg & Versteeg, supra note 16, at *14. This model was less popular than the business-as-usual model during the coronavirus pandemic. It was followed in Spain, Israel, Senegal, Hungary, and the Czech Republic, among others. Id., at *25.

[68] Gross, supra note 17 at 1021; Ferejohn & Pasquino, supra note 17, at 210-11. The U.S. Constitution does not contain an emergency clause (with the exception of the Suspension Clause, which grants the suspension power to Congress rather the President). However, scholars have argued that a similar process occurs as a political (instead of constitutional) response to emergencies. See Posner A. & Vermeule A. (2008) *The Executive Unbound: After the Madisonian Republic* Oxford.

[69] Bambauer & Ray, supra note 15, at 6.

responding to the crisis is "not concentrated but dispersed[70] and, consequently, there is no real value in suspending checks and balances. It follows that emergency regimes fail to minimize risks to civil rights, as is required *and possible* in a pandemic. As a legal matter, although the executive may be competent to adopt intrusive disease surveillance tools, the crude legal architecture of the emergency model cannot produce the required political legitimacy for it to do so. However, in a crisis in which wide public approval and cooperation are vital, legitimacy is the ultimate key to success.[71]

In sum, during a global, life-threatening pandemic, governments are expected to take *effective* and *justifiable* measures to save lives and prevent a calamity. This aim is best served neither by adopting a busines-as-usual stance nor by activating blanket emergency powers. Instead, the law governing response to pandemics should try to accommodate public health needs, while simultaneously placing stronger safeguards to minimize the impairment of rights.[72] An optimal balance of the individual rights and public interests at stake can only be struck after the effort to minimize the risks to rights of any measure is exhausted. This is the aim of the next section.

3.2. LEGAL AND INSTITUTIONAL DESIGN PROPOSALS

As a baseline, a digital contact tracing policy along the lines described above—high usage rates, location data collection, and greater capacity to exercise governmental control of the technology—requires an expansion of government power that should not be normalized, especially because it entails government surveillance of citizens and access to personal data that can be used for ill. This section outlines a legal architecture that attempts to accommodate these needs, while adopting several legal and institutional safeguards to minimize their costs.

[70] Ginsburg & Versteeg, supra note 16, at *20.

[71] This may have caused some countries to refrain from invoking constitutional emergency powers even though the formal conditions have been met. For example, the German government chose not to rely on Section 91 of the German Basic Law, which deals with internal emergencies. Instead, the government acted on an ordinary legislative tool— the Infection Protection Act of 2001.

[72] To keep the suggestions outlined in this section accessible to a wide audience from many jurisdictions, they are not framed around particular constitutional settings. In general, under U.S. law, the constitutionality of digital contact tracing will be evaluated under the requirements of the Fourth Amendment's reasonableness test. and in the "special needs" doctrine. Alan Rozenshtein has recently argued that government disease surveillance measures "would generally satisfy the Fourth Amendment." See Rozenshtein A. Z. (2021) 'Digital Disease Surveillance', Am. U. L. Rev. 70 [forthcoming]. Under the proportionality principle, used in many other countries as the frame for constitutional review, the question ultimately will be whether the social benefits advanced by DCT are proportionate to the infringement on protected rights. Minimization of the harm to privacy and other rights would be essential to show that the DCT measure is proportionate.

A framework health emergency statute. The first check against abuse of the power to conduct digital contact tracing is to confine it to restricted settings that are beyond government control. A combination of two types of checks will produce the optimal effect: legislative authorization and oversight, and reliance on scientific evidence. The standards and procedures governing DCT should be prescribed in a framework health emergency statute. The statute authorizes the employment of DCT upon the fulfillment of two conditions: first, a specific, time-limited legislative approval;[73] second, a triggering event, such as a pandemic declaration by the WHO,[74] or declaration of an epidemic endangering the health of the population by an independent scientific committee established by the law.[75] Each condition serves a different aim. The first ensures that significant tradeoffs between public safety and individual rights enjoy democratic legitimacy. As stated by the U.S. Supreme Court in another context, "[f]or reasons of inescapable human nature, the branch of the Government asked to counter a serious threat is not the branch on which to rest the Nation's entire reliance in striking the balance between the will to win and the cost in liberty on the way to victory."[76] Israel's Supreme Court embraced this approach in a case challenging an emergency regulation that authorized Shin-Bet (Israel's Security Agency) to conduct disease surveillance of Covid-19 contacts, holding that explicit statutory authorization is required as an "institutional safeguard that basic rights are not intruded unless strictly necessary."[77] The requirement that legislative approval be temporal (but renewable) guarantees that the legislature will continue to engage with the issue, while data assessing its success are aggregated. The second condition ensures that resort to such a drastic measure is grounded in scientific data. This type of justification adds another layer of legitimacy, one that rests on expertise and facts. Together, these checks guarantee that disease surveillance will not be normalized in the legal system.

The scope of authority. What should the legal authorization to deploy digital contact tracing include? The law should first specify the sources of data that are accessible to public health authorities and the technologies used for data collection. Location data may be collected from several sources, including electronic communication service providers,

[73] Cf., The General Security Service Enabling Law to assist in the national effort to reduce the spread of the new coronavirus and to promote the use of civilian technology to locate those who have been in close contact with patients (Temporary Order), 5720-2020 (hereinafter, Israel Disease Surveillance Law) (requiring a Parliamentary committee approval to enable the use og technological tools for digital disease surveillance).

[74] Cf., Bambauer & Ray, supra note 15, at 29.

[75] Cf., LOI n. 2020-290 du 23 mars 2020 d'urgence pour faire face à l'épidémie de covid-19, art. 3131-19 [Fr.] (requiring the assembly of a committee of scientists "without delay". The committee "periodically issues opinions on the state of the health disaster, the related scientific knowledge and the measures to put an end to it… as well as the duration of their application").

[76] Hamdi v. Rumsfeled 542 U.S. 507, 545 (2004) (Souter, J., concurring).

[77] HCJ 2187/20 Ben Meir v. Prime Minister, para. 31 (Apr. 26, 2020) [Isr.] (published in Heb.).

GPS-based apps, and scanning of QR-code upon entry to public places.[78] As mentioned above, it is preferable to enable a combination of location and proximity data to maximize accuracy, especially since location data can complement and assist manual contact tracing, while Bluetooth-based proximity tracing is more limited. The use of compulsory methods like the production of data from communication providers does not seem to provide substantial advantages. In Israel, for example, this system produced a high level of false positives and was able to find only about 10% of verified cases.[79] Therefore, preference should be given to smartphone apps that are more privacy preserving. The law should require that alternative technological solutions (e.g., cards, wearables) be available to people who lack access to smartphones. A centralized database will integrate identifiable data received from GPS, Bluetooth, and human interviews, subject to the safeguards listed below. This will produce accurate data that help locate contacts with maximum speed at minimum cost.

Another issue that should be addressed in the primary legislation is the type of consent required to join the program and the consequences of non-participation. Democratic countries have not favored mandatory participation, because of the ethical and legal implications for personal autonomy and privacy.[80] But the other extreme also bears costs. The European Data Protection Board guidelines, as well as the Google-Apple interface, mandate voluntary adoption of digital tracing tools and insist that "individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all."[81] This approach contributed to low usage rates and imposed public-health costs, although its privacy benefits compared to other, more moderate, options are uncertain. For example, it is unknown how many people who have not downloaded the apps did so out of concern for their privacy. There are reasons to believe that, for many people, other reasons, such as inertia or disbelief in the ability of the technology to slow down the virus, played a major role in the decision. A Pew Research Center report showed that 60% of Americans do not think that government disease surveillance can make a difference.[82] The irony is that this sort of skepticism is not a symptom of the limited value of digital contact tracing but a cause of it. Had more people participated in the programs, the tools would have been more useful. A vicious circle is thus maintained:

---

[78] To assist epidemiologic investigations, QR-based location data must be shared with public authorities. For example, Singapore mandates the use of a check-in system known as SafeEntry that requires users to scan a QR code upon entry to workplaces and other public facilities and transmits the data to public health authorities.

[79] The Privacy Protection Authority, Memorandum No. 10 (submitted in accordance with sec. 12 of Israel Disease Surveillance Law, supra note 73) (4 Jan. 2021) (Heb.) https://www.gov.il/BlobFolder/reports/privacy-shabak-coronavirus_10/he/op_shabak_10.pdf.pdf

[80] MIT Covid Tracing Tracker, supra note 12.

[81] See EDPB Guidelines, supra note 31, at 7.

[82] Pew Res. Ctr., More Americans think location tracking through cellphones won't make a difference in limiting the spread of COVID-19 than say it would help (16 Apr. 2020). https://www.pewresearch.org/fact-tank/2020/04/16/most-americans-dont-think-cellphone-tracking-will-help-limit-covid-19-are-divided-on-whether-its-acceptable/ft_2020-04-16_cellphonetracking_01a/

low adoption rates cause the technology to be less effective, and the limited effectiveness discourages people from signing on.

It is helpful to think of the problem of consent through the frame of minimalization: what type of participation regime would be *useful* at *minimum cost* to privacy and autonomy? One possibility is 'opt-out' participation: the technology is automatically enabled in smartphones and other devices, but people who strongly prefer not to take part in the program are able to withdraw. This architecture incorporates those who act on inertia or who don't care that much about privacy to assume the burden of signing out, thus raising adoption rates without imposing real harms to privacy.[83] Another option is restricting access to public facilities (workplaces, government buildings, shopping malls, etc.) to those who refuse to participate. This regime may require public places to maintain registration of visitors via QR-codes or beacons that automatically record devices within their range. People who do not download the app will be able to access certain public facilities only at limited times and are thus subject to tighter restrictions on movement. Contrary to the European guidelines, this regime disadvantages people for not using the technology.[84] But its logic is no different than face mask mandates that in countries like Spain, France, and Israel, are universal in public settings.[85] Ethically, this regime can be justified on a principle of non-reciprocal risk: when people engage each other in a public space, an individual who is unwilling to download the app (and thus avoid the added risk on her privacy) is imposing a non-reciprocal health risk on an individual who has downloaded the app.[86] It is thus normatively appropriate to deprive the first individual of equal access to work, commerce, and public services.

Finally, the framework statute should address the problem of big-tech tyranny: how can governments ensure that their preferred DCT policy will not be blocked by software and hardware architecture dictated by technology companies? This is a delicate issue. Much like other tradeoffs in the debate about digital contact tracing, there is no clear 'right' answer. While it is important that the economic interests of private actors not hinder the use of technology to limit the spread of infectious diseases, there are reasons to think that some constraints imposed by the private sector are desirable.[87] Moreover, the enactment of a framework statute with adequate safeguards might facilitate public-private cooperation and decrease the tendency of tech companies to resist government action. Until this becomes a significant issue, it may be preferable to avoid regulation of

[83] For an ethical analysis of opt-out digital contact tracing see Mello M.M. & Wang C.J. (2020) 'Ethics and Governance for Digital Disease Surveillance', *Science* 368, 951:6494, 951-54.

[84] Supra note 31.

[85] Note that mask mandates in various forms are enforced in many countries. See Felter C. & Bussemaker N. (2020) 'Which Countries Are Requiring Face Masks?' *Council on For. Rel.*, 4 Aug. https://www.cfr.org/in-brief/which-countries-are-requiring-face-masks

[86] Cf. Fletcher G.P. 'Fairness and Utility in Tort Theory', *Harv. L. Rev*. 85 537:573.

[87] Cf. Rozenshtein, supra note 57 (describing how tech companies constrain the government's power to conduct national security surveillance; arguing that this function enhances the separation of powers).

companies in this area. States vary in their ability to strong-arm the world's largest tech companies, and forcing changes in architecture might require states to coordinate their strategy. With these caveats, I think that lawmakers should consider strategies to deal with a situation in which a policy deemed vital for promoting public health is impeded by private firms. As Andrew Woods explains, regulatory efforts may be costly when the big tech companies flex their muscles, but "the state is still the final word."[88] To counter dire health emergencies, governments should be willing to assert their sovereign power.

Safeguards. To minimize the risks to rights, the grant of authority to conduct digital conduct tracing should be subject to adequate safeguards. As noted above, health emergencies are more amenable than national security emergencies to robust checking by courts, legislative bodies, and the public.[89] Establishing substantive and procedural safeguards is both feasible and highly effective for ensuring maximum public health benefits at minimum social cost. What should these safeguards include?

First, strict *purpose limitation*. Data collected must only be used for epidemiological analysis and not for any other purposes, such as law enforcement.[90] This is vital to ensure that an emergency power does not creep to matters unrelated to the emergency. Second, under the principle of *data minimization*, the legal and technical design must ensure that authorities collect the "the narrowest possible set of data elements"[91] required, with minimal impairment of privacy and data security.[92] The processing of contacts should be commenced only upon confirming infection and, until then, data should be encrypted and stored locally on the device. Data shared with health authorities must be kept safely, for limited duration, and not disclosed to third parties.[93] Upon termination of the legal authorization, all data must be deleted. Unauthorized decryption should constitute a criminal offense.[94] Third, ***data subjects' rights*** should be specified in the primary legislation. A person must receive access to data collected and processed from her device and be able to petition to delete data upon showing an overriding interest. Fourth, an institutional culture of *transparency* should be embedded in the program. Public health authorities must be required to periodically produce full information to the relevant executive and legislative bodies, and this reporting should be

[88] Woods A.K. (2019) 'Tech Firms Are Not Sovereigns', p. 4-5 *Hoover Inst.* https://www.hoover.org/sites/default/files/research/docs/woods_webreadypdminimize the rf.pdf.

[89] See supra notes 69-71 and accompanying text.

[90] Some have argued for allowing exceptions to this principle in extreme situations involving imminent risk of serious physical injury. See Rozenshtein, supra note 72, at *47.

[91] Mello & Wang, supra note 83, at 953.

[92] The principle of data minimization is central to the E.U. data protection legal framework. For an overview in the context of COVID -19 see E.U. Commission, Guidance on Apps Supporting the Fight Against COVID-19 Pandemic in Relation to Data Protection (App Guidance), para 3.4, 2020 O.J. (C. 124 I).

[93] Cf. Hamagen ('the Shield') app Privacy Policy and Information Security (Isr.) (Jan. 21, 2021) https://govextra.gov.il/ministry-of-health/hamagen-app/magen-privacy-en/ (providing that information shared with authorities and not used for epidemiological investigations will be deleted within 30 days").

[94] Cf. Privacy Amendment (Public Health Contact Information) Act 2020, art. 94G [Australia].

made available to the public. Transparency will enable effective oversight, inform legislative deliberations on extending or terminating the program, and ensure accountability.[95] In addition, the app's source code "should be made publicly available for the widest possible scrutiny."[96]

Fifth, *appeals rights*. Identified contacts may be required to self-quarantine. To minimize harm resulting from false positives, an *administrative appeals mechanism* should be established. Persons identified as having been in contact with confirmed patients must be able to appeal and have their case reviewed promptly. In Israel, where nationwide disease surveillance is enforced, individuals who believe their quarantine notification was sent in error can dispute the decision online or through a 24/7 hotline and receive a timely ruling.[97] An efficient appeals mechanism encourages greater adherence to quarantine notifications and increases public trust in the program. Finally, policy and individual decisions under the program should be subject to *judicial review*. Courts are uniquely capable of guarding against abuse and unfairness, as well as resolving separation of powers issues between the political branches if they arise.[98]

CONCLUSION

Effective digital contact tracing imposes risks on privacy, autonomy, and data security. These risks can be significantly reduced, but not eliminated, by the recommendations for legal and institutional design outlined in this essay. This leaves the question of whether digital contact tracing should be pursued at all: is it worth the sacrifices? As noted earlier, it is debatable whether there is an objectively 'right' answer to this question. But the creation of public policy is always a choice between imperfect alternatives, and any policy choice can only be assessed against possible alternatives. Here, the alternatives involve serious implications on rights and vital public interests. Manual contact tracing also intrudes on privacy, sometimes even more than technological measures. In a pandemic of this scale manual contact tracing cannot suppress community transmissions by itself, which means that harms resulting from mass lockdowns, restrictions on the freedoms of movement, work, worship, and assembly, closure of businesses, increased illness, and loss of life are aggravated. These harms tend to disproportionately disadvantage vulnerable groups, including the elderly, the poor, and people with chronic health problems.

---

[95] Cf. Israel Disease Surveillance Law, supra note 73, at Sec. 19.

[96] EDPB Guidelines, supra note 31, at 8.

[97] See Ministry of Health, Open a dispute over an isolation order [Isr.] https://www.gov.il/en/Departments/Guides/corona-quarantine?chapterIndex=11#appeal

[98] Cf., HCJ 2187/20 Ben Meir v. Prime Minister (Apr. 26, 2020) [Isr.] (published in Heb.) (holding that disease surveillance by the ISA must be authorized in primary legislation).

There can be little doubt that effective digital contact tracing can be an important building block on a pandemic response that reduces societal harms. All in all, I think that the net effect of digital contact tracing, as envisioned in this essay, is also the least restrictive measure on human rights.

REFERENCES

Albergotti R. & Harwell D. (2020) 'Apple and Google are building a virus-tracking system. Health officials say it will be practically useless,' Wash. Post, 15 May. https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/

Bambauer J. et al. (2020) 'It's Time to Get Real About COVID Apps, Fighting Covid with Data working grp., 14 May. https://medium.com/@DataVersusCovid/its-time-to-get-real-about-covid-apps-dd82e08895f2

Bambauer J. & Ray B. (2020) 'Covid-19 Apps are Terrible—They Didn't Have to be,' *The Digital Social Contract: A Lawfare Paper Series*

Barigazzi J. (2020) 'WHO COVID envoy warns of third wave in Europe in 2021', *Politico*, 22 Nov. https://www.politico.eu/article/coronavirus-third-wave-europe-2021-world-health-organization-envoy/

Barak A. (2012) *Proportionality: Constitutional Rights and their Limitations*, Cambridge

Barry E & DePasquale R. (2020) 'Officials scale back contact tracing efforts in the U.S., saying they cannot keep up', *N.Y. Times Corona Virus Live Update*, 30 Nov. https://www.nytimes.com/live/2020/11/24/world/covid-19-coronavirus#officials-scale-back-contact-tracing-efforts-in-the-us-saying-they-cannot-keep-up

Benjamin G. C. (2020) 'The Secret Weapon Against Pandemics', *TED2020*, 20 May. https://www.ted.com/talks/georges_c_benjamin_the_secret_weapon_against_pandemics/transcript

Calo R. (2020) 'Enlisting Big Data in the Fight Against Coronavirus, written testimony before the Senate Committee on Commerce, Science, and Transportation, at 3, 9 Apr. https://www.commerce.senate.gov/services/files/D069F0C0-2B67-4999-AC75-5BC41D14D00C

Cellan-Jones R. (2020) 'Coronavirus: What went wrong with the UK's contact tracing app?', *BBC News*, 20 Jun. https://www.bbc.com/news/technology-53114251

De la Garza A. (2020) 'People Are Finally Downloading COVID-19 Exposure Notification Apps. Will They Make a Difference?,' *Time,* Dec. 14. https://time.com/5921518/covid-exposure-notification-apps/

Ferejohn J. & Pasquino P. (2004) 'The Law of the Exception: A Typology of Emergency Powers', Intl J. Con. L. 2, 210:239

Felter C. & Bussemaker N. (2020) 'Which Countries Are Requiring Face Masks?' *Council on For. Rel.*, 4 Aug. https://www.cfr.org/in-brief/which-countries-are-requiring-face-masks

Ferretti L. et al. (2020) 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing', *Science* 368

Fletcher G.P. 'Fairness and Utility in Tort Theory', *Harv. L. Rev*. 85 537:573

Ginsburg T. & Versteeg M (2020) 'The Bound Executive: Emergency Powers During the Pandemic' (Jul. 26, 2020) Virginia Public Law and Legal Theory Research Paper No. 2020-52, U of Chicago, Public Law Working Paper No. 747, Available at SSRN: https://ssrn.com/abstract=3608974

Gray S. (2020) 'Enlisting Big Data in the Fight Against Coronavirus, written testimony before the Senate Committee on Commerce, Science, and Transportation,' at 35-36, 15 Apr.

Gross O. (2003) 'Chaos and Rules: Should Responses to Violent Crises Always Be Constitutional?' Yale L.J. 112, 1011:1134, 1043:58

Hecht-Felella L. & Mueller-Hsia K. (2020) 'Rating the Privacy Protections of State Covid-19 Tracking Apps,' *Brenan Ctr. for Justice* (Nov. 5, 2020) https://www.brennancenter.org/our-work/research-reports/rating-privacy-protections-state-covid-19-tracking-apps

Hinch R. et al. (2020) 'Effective Configurations of a Digital Contact Tracing App: A report to NHSX', at *9, 16 Apr.

Kharpal A. (2020) 'Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends', *CNBC*, 30 Mar. https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html

Kissick C. et al. (2020) 'What Ever Happened to Digital Contact Tracing?' *Lawfare*, 21 Jul. https://www.lawfareblog.com/what-ever-happened-digital-contact-tracing

Kretzschmar M. et al. (2020) 'Isolation and Contact Tracing Can Tip the Scale to Containment of COVID-19 In Populations with Social Distancing', 23 Mar. Available at SSRN: https://ssrn.com/abstract=3562458

Law Library of Congress (2020) 'Regulating Electronic Means to Fight the Spread of COVID-19,'

Leith D. J. & Farrell S. (2020) 'Coronavirus Contact Tracing: Evaluating the Potential of Using Bluetooth Received Signal Strength for Proximity Detection,' *ACM SIGCOMM Computer Communication Rev.* 50

Lewis D (2020) 'Where COVID Contact Tracing Went wrong', *Nature* 588 384-388 (Dec. 2020)

Long C. (2020) *Privacy and Pandemics, in Law in the Time of Covid-19* (Pistor K. ed.) [online]

Mello M.M. & Wang C.J. (2020) 'Ethics and Governance for Digital Disease Surveillance', *Science* 368, 951:6494, 951-54

Milsom L. et al., Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy (Jul. 2020) https://osf.io/7vgq9/

O'Neill P. H. (2020) 'Google and Apple ban location tracking in their contact tracing apps', *MIT Tech. Rev.*, 4 May. https://www.technologyreview.com/2020/05/04/1001060/google-and-apple-lay-out-rules-for-contact-tracing-apps/

Park A. (2020) 'The Tech That Could Be Our Best Hope for Fighting COVID-19—and Future Outbreaks', *Time*, 19 Mar., https://time.com/5805622/coronavirus-pandemic-technology/

Park S. et al. (2020) 'Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies', *J. Am. Med. Association* 323 2129:2130

Perera D. (2020) 'South Carolina legislature puts coronavirus apps on hold,' M.Lex, 26 Jun. https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/south-carolina-legislature-puts-coronavirus-apps-on-hold

Posner A. & Vermeule A. (2007) Terror in the Balance: Security, Liberty, and the Courts, Oxford

Posner A. & Vermeule A. (2008) *The Executive Unbound: After the Madisonian Republic* Oxford

Raskar R. et al. (2020) 'Adding Location and Global context to the Google/Apple Exposure Notification Bluetooth API,' Eprint arXiv:2007.02317 [cs.CR], 25 Jul. https://arxiv.org/abs/2007.02317

Robinson A. & Waldo J. (2020) 'Technical Difficulties of Contact Tracing,' *Lawfare*, 17 Dec. https://www.lawfareblog.com/technical-difficulties-contact-tracing

Rossiter C. (1948) *Constitutional Dictatorship: Crisis Government in the Modern Democracies* Princeton

Rozenshtein A. Z. (2021) 'Digital Disease Surveillance', Am. U. L. Rev. 70 [forthcoming]

Rozenshtein A. Z. (2018) 'Surveillance Intermediaries,' Stan. L. Rev. 70 99:189

Scott M. et al. (2020) 'How Google and Apple outflanked Governments in the Race to Build Coronavirus Apps', *Politico* (May 15, 2020, 5:25 AM) https://www.politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/

Schneier B., Me on COVID-19 Contact Tracing Apps,' *Schneier on Security*, 1 May. https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html

Schumaker E. (2020) 'Apple and Google launch digital contact tracing system, *ABC News*, 6 May. https://abcnews.go.com/Technology/apple-google-launch-digital-contact-tracing-system/story?id=70789376

Sharon T. (2020) 'Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers,' Ethics and Info. Tech. 2020, 1:13

Shead S. (2020) 'In Major U-turn, the UK will now use Apple and Google's Platform for its Coronavirus Tracing App', *CNBC*, 18 Jun. https://www.cnbc.com/2020/06/18/apple-and-googles-tech-to-underpin-uk-contact-tracing-app.html

Shwartz Altshuler T. & Aridor Hershkovitz R. (2020) 'Coronavirus: Israeli and Comparative Perspectives', *Brookings Inst*

Stanley J. & Granick J. (2020) 'The Limits of Location Tracking in an Epidemic, *ACLU*, at 3-4, 8 Apr. https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf

Valentino-DeVries J. (2020) 'Coronavirus Apps Show Promise but Prove a Tough Sell,' *N.Y. Times* Dec. 7. https://www.nytimes.com/2020/12/07/technology/coronavirus-exposure-alert-apps.html

Simko L. et al. (2020) 'COVID-19 Contact Tracing and Privacy: Studying Opinion and Preferences,' *U. Wash. Security Lab Covid-19 Relate Res.* (Rep. Ver. 1.0) 8 May

Woods A.K. (2019) 'Tech Firms Are Not Sovereigns', p. 4-5 *Hoover Inst.* https://www.hoover.org/sites/default/files/research/docs/woods_webreadypdminimize the rf.pdf

Zuboff S. (2019) *The Age of Surveillance Capitalism*, Profile