2022

Secrecy Nurtures Disease: Balancing Privacy Concerns with COVID-19 Contact-Tracing Measures

Julianna Dzwierzynski

Secrecy Nurtures Disease: Balancing Privacy Concerns with COVID-19 Contact-Tracing Measures

Julianna Dzwierzynski*

I. Introduction

In December 2019, the novel coronavirus disease ("COVID-19") first emerged in Wuhan, China and rapidly progressed to a global pandemic by early 2020.[1] To date, over one hundred and fifteen million cases have been reported and over two and a half million deaths have been recorded globally.[2] In the United States alone, more than 32,736,063 people have been infected and at least 581,302 have died.[3] As conditions worsen and case numbers continue to spike, American life has been fundamentally altered. In an effort to help slow the spread of COVID-19 around the world, various digital contact-tracing measures have emerged.

Contact tracing is a method to delay the spread of infectious diseases.[4] Traditionally, in communities utilizing contact tracing, hospitals and labs send names of individuals who have been recently diagnosed with COVID-19 to local health departments.[5] The health department then notifies others who may have been exposed to the virus as a result of being in close proximity with the infected individual.[6] COVID-19 patients are often contagious despite being asymptomatic,

* J.D. Candidate, 2022, Seton Hall University School of Law; B.A., Marquette University.

1 *Identifying the Outbreak Source*, CTR. FOR DISEASE CONTROL AND PREVENTION (July 1, 2020), https://www.cdc.gov/coronavirus/2019-ncov/cases-updates/about-epidemiology/identifying-source-outbreak.html.

2 Johns Hopkins University of Medicine Coronavirus Resource Center, https://coronavirus.jhu.edu/map.html (Last updated Mar. 4, 2021).

3 *Coronavirus in the U.S.: Latest Map and Case Count*, N.Y. TIMES (May. 10, 2020), https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html.

4 William F. Marshall, *Contact tracing and COVID-19: What is it and How Does it Work?*, MAYO CLINIC (Nov. 3, 2020), https://www.mayoclinic.org/diseases-conditions/coronavirus/expert-answers/covid-19-contact-tracing/faq-20488330.

5 *Id.*

6 *Id.*

accelerating its transmissibility.[7] As COVID-19 spreads rapidly, the time consuming and labor-intensive traditional methods of contact tracing proved to be insufficient in managing the increase of cases. Tech giants, like Apple and Google, have partnered with public health authorities across the globe to build application programming interfaces ("APIs"), as a modern enhancement to track the spread of the virus, find new infections, and support the reopening of global economies.[8] While most countries promptly implemented some form of a contact tracing app, such apps have made slow progress throughout the United States.[9] According to public-health experts, part of the problem has been lack of coordination by the federal government, wariness of investing resources in an unproven solution, and an overarching lack of trust in technology companies.[10]

These apps pose several privacy threats related to potential overreach, discrimination, and voluntariness. Moreover, developers have not yet addressed whether an exit strategy exists to sunset the data after the pandemic ends. The escalation of the pandemic has raised questions about whether governments are prepared to navigate these various privacy issues as they take on greater roles in collecting individuals' data.[11]

The global pandemic is not a singular problem with a perfect solution. Rather, how governments operate through technology is integral in addressing the public health crisis. If governments are to operate through technology, they must acknowledge the limitations of accountability in technology as we put civil and political liberties on the line. In balancing the

---

[7] Seyed M. Moghadas et al., *The Implications of Silent Transmission for the Control of COVID-19 Outbreaks*, 30 PNAS 1, 1 (2020) ("Silent disease transmission during the presymptomatic and asymptomatic stages are responsible for more than 50% of the overall attach rate in COVID-19 outbreaks.").
[8] Jessica Davis, *COVID-19 Contact Tracing Apps Spotlight Privacy, Security Rights*, HEALTH IT SECURITY (May 20, 2020), https://healthitsecurity.com/news/covid-19-contact-tracing-apps-spotlight-privacy-security-rights.
[9] Alejandro de la Garza, *Contact Tracing Apps Were Big Tech's Best Idea for Fighting COVID-19. Why Haven't They Helped?*, TIME (Nov. 10, 2020, 7:00 AM), https://time.com/5905772/covid-19-contact-tracing-apps/.
[10] *Id.*
[11] *See generally* Aaron J. Burnstein, *Privacy and Data Use in U.S. Government Responses to COVID-19*, AM. BAR ASS'N: ANTITRUST (Summer 2020), https://www.americanbar.org/digital-asset-abstract.html/content/dam/aba/publishing/antitrust_magazine/atmag-summer2020/smmr20-burstein.pdf.

integral nature of contact tracing apps to track and stop the spread of COVID-19 (or future pandemics) with the various privacy concerns they involve, this Comment will propose that the best solution is for state governments to adopt a voluntary use of a less invasive, decentralized model and place limitations on data storage periods. Governments need to be transparent about the gaps in data and the mechanisms for ensuring systems are not being built on inaccurate data. Moreover, in constructing an exit strategy for stored data, state governments and app developers must implement a means to guard against function creep, ensuring our data is relevant to the current state of affairs in terms of public health and safety during COVID-19. While use of data for research could be useful in the long term, we need to balance the need for research purposes with stricter controls of data deletion after a certain period of time.

Part II of this Comment takes a historical look at contact tracing and explores the development of both the centralized and decentralized models of digital contact-tracing apps. Additionally, Part II will examine comparative contact-tracing models used in other countries. Part III explains the various privacy threats that digital contact-tracing apps implicate including overreach, anonymity, location tracking, voluntariness, consent, technological limitations, and exit strategy. Part IV examines current privacy law as it has developed since the HIV/AIDS crisis and location tracing law. Finally, Part V proposes what changes should be made to privacy law to address the unique situation of these apps with regard to COVID-19 and with regard to future pandemics. Ultimately, this Comment will argue that these apps pose grave privacy threats that can be alleviated by state governments partnering with tech developers to institute a decentralized app that encourages participation to combat the spread of COVID-19.

II. Different Application Models

In Part I, this Comment first establishes the basic history of contact tracing and its transition to a digital format in the wake of the coronavirus pandemic. Then this section will describe the differences between the centralized and decentralized application models and the benefits and downfalls of both. Further, this section will elaborate on the unveiling of the Google/Apple partnership and how their development of the Exposure Notification System ("ENS") works to enable a broader Bluetooth-based contact tracing platform as a more robust solution than an API and would allow more individuals to participate if they choose to opt-in. Finally, this section will describe various contact-tracing models and mass surveillance applications used in other countries.

A. History of Contact-Tracing

Contact tracing is a well-established and essential tool for public health officials to combat the spread of infectious diseases.[12] Historically, contact tracing has been conducted through the efforts of skilled workers who conduct interviews, contact at-risk individuals, and counsel individuals through a quarantine period, if necessary.[13] Contact tracing refers to "the process of identification of contacts who may have come in contact with an infected victim and subsequent collection of further information about these contacts."[14] In practice, contact tracing is performed for a variety of diseases: sexually transmitted infections (including HIV) and viral infections.[15] The overall purpose of contact tracing as a solution is two-fold. First, at a global level, contact-tracing aids

[12] Hyunghoon Cho et al., *Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs*, at 1 (2020), https://arxiv.org/pdf/2003.11511.pdf; *see also* Leonie Reichert et al., *Privacy-Preserving Contact Tracing of COVID-19 Patients* (2020), https://eprint.iacr.org/2020/375.pdf ("Contact tracing deals with finding unreported infected people by tracing back who could have possibly caught the disease from a verified case.").
[13] Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID-19*, 7 J. LAW BIOSCI 1, 11 (2020).
[14] Qiang Tang, *Privacy-Preserving Contact Tracing: Current Solutions and Open Questions*, at 4 (2020), https://eprint.iacr.org/2020/426.pdf
[15] *Id.*

medical personnel in tracing the origin and pattern of the virus to take appropriate actions and craft strategies (i.e., enforcing social distancing, lockdowns, etc.) to fight against the virus and future pandemics.[16] Second, at an individual level, contact-tracing aids medical personnel in alerting specific individuals who are at risk of infection and allow them to evaluate how to take further action.[17] Given the unique attributes of COVID-19 and its ability to be spread either through direct or indirect contacts, recent modelling data comparing traditional methods of contact tracing and those of digital contact tracing have indicated that COVID-19 spreads too quickly to be controllable through traditional methods.[18] In contrast, digital contact tracing may be overbroad and too impersonal, rendering it a less effective means than traditional contact-tracing in generating compliance.[19]

B. Fragmented U.S. Strategy

Particularly in the U.S., in the absence of a unified federal strategy, tracing efforts lag and the country leads the world with over 32.5 million infections and 581,302 deaths.[20] Without a national strategy, states are required to take their own approaches. At least twenty states developed their own contact-tracing apps to supplement deficiencies in traditional contact-tracing capabilities.[21] Many states, however, refuse to develop contact-tracing apps in response to privacy concerns.[22]

---

[16] *Id.* at 5.
[17] *Id.*
[18] Ram & Gray, *supra* note 13, at 10; *see also* Reichert, *supra* note 12, at 1 ("The current COVID-19 pandemic shows the necessity to automate contact tracing to quickly discover new infections and slow down the spreading."); Devin Skoll et al., *COVID-19 Testing and Infection Surveillance: Is a Combined Digital Contact-Tracing and Mass-Testing Solution Feasible in the United States?*, 1 CARDIOVASCULAR DIGITAL HEALTH J. 149, 153–54 (2020) ("Contact tracing alone is insufficient to control COVID-19 transmission without complementary large-scale testing to identify COVID-19 carriers . . . increasing the frequency of testing would improve accuracy while less expensive equipment would expand its distribution to identify more cases, thus accelerating the speed of results required to prompt individuals to quarantine without delay.").
[19] Ram & Gray, *supra* note 13, at 11–12 ("[D]epending on precision of location data, prompts to self-isolate may become overbroad and routine, which will further reduce compliance.").
[20] *Coronavirus in the U.S.: Latest Map and Case Count*, N.Y. TIMES (May. 10, 2020), https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html.
[21] *Id.*
[22] *Id.*

The gaps at both the national and state levels have prompted cities and private corporations (i.e., Uber and university systems) to develop their own contact-tracing strategies, further fragmenting the system and inhibiting the Department of Health's ability to adequately combat COVID-19.[23] The U.S. public demonstrates wariness in embracing these new digital developments putting possible public health gains second to the loss of privacy and civil liberties.[24] The fragmented implementation of contact-tracing apps, public wariness over privacy concerns, and lack of testing/manual contact-tracing casts doubt on whether the U.S. will be able to successfully employ technology produced by its own technology giants.[25]

C. Centralized (Data-First) versus Decentralized (Privacy-First)

Worldwide, approximately eighty contact tracing apps have been developed to combat COVID-19 by tracking when two devices come into close contact with one another.[26] One of the most salient differences in development of these various models is the divide between "data-first" models which "prioritize the retention of tracking data and its availability to health authorities and researchers," and "privacy-first" approaches, which emphasize individuals' "control over their own data and seek to provide an effective degree of contact tracing without exposing identifiable individuals' movements and interactions to authorities."[27] At the most basic level, functionality of these approaches is the same in that "an alert can be issued across the network when an individual tests positive for COVID-19," either by direct alert from health authorities or by the

[23] *Id*.
[24] *Id*. at 5 ("In a June 2020 survey from Avira, 71% of Americans did not plan to download a contact-tracing application, citing privacy as a primary concern, and there is an ideological opposition by some to any form of tracing. Much of this stems from concern about data safety and long-term use.").
[25] *Id*.
[26] Samual A. Garner, *US Privacy Law and Contact Tracing Apps: Considerations for Mitigating Risk*, BCLP (July 6, 2020), https://www.bclplaw.com/en-US/insights/us-privacy-law-and-contact-tracing-apps-considerations-for-mitigating-risk.html.
[27] Robert A. Fahey & Airo Hino, *COVID-19, Digital Privacy, and the Social Limits on Data-Focused Public Health Responses*, 55 INT'L J. INFO. MGMT 1, 2 (2020).

individual who tested positive for COVID-19 entering a particular code on their device (i.e. smartphone) to alert anyone who may have been exposed.[28]

Apart from this most basic function, the design of the two different applications diverges in how they identify and contact individuals who come in contact with the virus. The centralized or "data-first" model allows health authorities to directly identify and contact potentially exposed individuals.[29] Alternatively, the decentralized or "privacy-first" model does not identify individuals who opt-in and only notifies them on their smartphones, leaving the decision to get tested in the hands of the individual.[30]

The centralized approach is designed to gather the anonymous phone ID code of someone who has tested positive as well as the ID codes of their close contacts and deposit all information in a central server that is operated by the government and protected by cybersecurity measures to conduct contact-tracing, perform analysis, and generate necessary alerts.[31] In this structure, an individual user must sign up to central server which automatically creates a "privacy-preserving Temporary ID (TempID)[32] for each of the registered devices."[33] Devices exchange these private TempIDs through "Bluetooth encounters messages" as they pass by one another or come into close contact.[34] Then, if a user tests positive for COVID-19, the server maps the TempIDs from all Bluetooth encounter messages to detect contacts that may be at risk.[35] This centralized approach appears to be an invaluable resource for data scientists and health officials researching COVID-19

[28] *Id*.
[29] *Id*.
[30] *Id*.
[31] Skoll, *supra* note 18, at 153.
[32] This TempID is encrypted with a key known only to the central server's authority.
[33] Molla R. Hussein et al., *Digital Surveillance Systems for Tracing COVID-19: Privacy and Security Challenges with Recommendations* 2 (July 26, 2020) (unpublished manuscript).
[34] *Id*.
[35] *Id*.

and mechanisms to manage future epidemics more generally.[36] While this method enables health officials to "view networks of contacts and better identify super spreaders," as it generates a large quantity of data on the movement of and contacts between individuals, it also puts individuals at risk for data breaches and potential overreach as "data enables future possibility of state surveillance."[37]

The decentralized model, on the other hand, is designed such that only an individual user's ID is sent to a centralized database and the phone then downloads data and content matches locally.[38] In other words, the decentralized model gives users more control over their information. A higher degree of privacy is implemented as the database of users who have tested positive is routinely downloaded onto a smartphone, and if a match occurs, the user then receives an exposure notification directly to their phone.[39] The decentralized model serves as a "bulletin board" for the required lookup of exposure information, ensuring user privacy by creating anonymous identifiers inside smartphones or other user devices—keeping real identities secret from both the central server and other users.[40] While decentralized apps remedy concerns about user privacy, their function can hinder the broader effect of contact tracing. Keeping contacts anonymous in this way hinders progress by health officials in assuring the correct people are getting notified.[41]

---

[36] Fahey & Hino, *supra* note 27.
[37] Skoll, *supra* note 18, at 150; *see also* Young E. Saw et al., *Towards a Digital Solution: Predicting Public Take-up of Singapore's Contact Tracing Mobile Application During the COVID-19 Crisis* (Sept. 1, 2020) ("Although this method comes with costs to users' privacy, it enables public health agencies to detect community spread.").
[38] Skoll, *supra* note 18, at 150.
[39] Saw, *supra* note 37; *see also*, Elissa Redmiles, *Concerns and Tradeoffs in Technology-Facilitated Contact Tracing*, 2 DIGITAL GOV'T: RES. AND PRACTICE 1, 2 (2020) ("[U]sers' apps periodically generate anonymized identifiers for them, which are broadcast to other apps within a given distance at periodic time intervals. Apps whose users have reported that they have tested positive for COVID-19 push a list of exposed contact identifiers to a public list . . . the other decentralized apps periodically pull this public list and check if they have any matches; if so, they notify the user that they have been exposed.").
[40] Hussein et al., *supra* note 33.
[41] Skoll, *supra* note 18, at 150.

On April 10, 2020, Google and Apple announced their joint effort to construct a decentralized ENS contact-tracing application for iPhone and Android devices.[42] The Apple/Google API responded to the several of the gravest privacy concerns by combining random identification numbers so no personally identifiable data is exchanged, an opt-in system to acquire consent, and utilizing a decentralized model to store and process data on users' devices.[43] This ENS system enables apps made by national public health authorities to use Bluetooth in the background such that when "phones come into contact, each phone generates a random numerical ID that it broadcasts to nearby phones" to preserve anonymity.[44] The Apple/Google partnership posited a design that had desirable security properties. Rather than tracking users' location, the ENS app uses Bluetooth signal to connect with nearby devices.[45] Moreover, Google and Apple are using better encryption methods by scrambling identifying information and protecting any potentially identifiable information related to the device.[46] Apple and Google have stated that "only apps designated by public health authorities will have access to this framework and such apps must meet specific criteria around privacy, security, and data control."[47] The tech giant duo rebranded their voluntary app as an "exposure notification system" rather than a contract-tracing solution and made promises to dismantle the system at the end of the pandemic.[48] Several privacy researchers cautiously welcomed the new ENS framework as it "provided assurances over short-term COVID-

[42] Laura Bradford, *COVID-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*, 7 J. L. BIOSCI 1, 2 (2020).
[43] Tamar Sharon, *Blind-sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers*, at 3 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7368642/pdf/10676_2020_Article_9547.pdf.
[44] Skoll, *supra* note 18, at 150.
[45] Garner, *supra* note 26; *see generally* Nicole Martinez-Martin et al., *Digital Contact Tracing, Privacy, and Public Health*, Hastings Center Report, (May-June 2020) (explaining the general concept behind use of Bluetooth technology to register proximity between phones of people diagnosed with COVID-19 and other smartphone users).
[46] Garner, *supra* note 26.
[47] Bradford, *supra* note 42, at 3.
[48] Garner, *supra* note 26.

19 surveillance and centralized data breach concerns," but they were "wary of the obviously unchecked and potentially uncheckable power of these platforms."[49]

The ENS framework generates and collects four types of information: (1) Bluetooth identifier codes and associated contact event information; (2) positive diagnosis information; (3) associated information (when an individual notifies via the app that they have the virus, their individual IP address and other metadata will be detectable); and (4) notifications to exposed users.[50] A potential fifth category of data collection includes gathering "a combination of the exposure data collected by the apps using the Google/Apple ENS with individual user identities and location data in order to (1) assist law enforcement to ensure quarantine of infected and/or exposed individuals; (2) use location data in aggregate to track the spread of the virus across a population; or (3) use individual exposure data to make inferences about health."[51] Apple and Google, however, designed their ENS framework to make automated collected of this last category extremely difficult.[52]

D. Comparative Models

While it is hopeful that the ENS framework accelerates progress with regards to generating and tracking COVID-19 information, several other countries were quick to adopt their own models. Some countries like China, South Korea, Israel, and Singapore quickly adopted systems that fail to take their citizens' privacy into consideration.[53] China initially adopted a variety of tools to contain the spread of COVID-19 including the mandated use of a mobile smartphone application (Health Code), which generates a rating indicating the likelihood of an individual's

[49] MICHAEL VEALE, SOVEREIGNTY, PRIVACY, AND CONTACT TRACING PROTOCOLS; DATA, JUSTICE, AND COVID-19 34 (L. Taylor et al. eds., 2020).
[50] Bradford, *supra* note 42, at 4.
[51] *Id*.
[52] *Id*.
[53] Reichert, *supra* note 12.

exposure to the virus and dictates whether individuals can walk freely or not.[54] Additionally, there are hundreds of millions of cameras equipped with facial recognition to enable contact tracing efforts and identify quarantine violations.[55] China's mass surveillance program combined with mass testing has been greatly effective in preventing a second wave of infections.[56]

In South Korea, the government has maintained a public database of known COVID patients, which includes information about their age, gender, occupation, and travel routes.[57] South Korea responded to COVID by transparently communicating information through emergency phone alerts which contained details of new cases. Citizens who were willing to wear masks and cooperate with contact tracers accepted this system and acknowledged privacy would be a requisite tradeoff.[58] Moreover, the epidemiological intelligence officers monitor GPS data, CCTV footage, credit card transaction data, and travel information to ensure that infected individuals or those under ordered quarantine would comply.[59]

Israel, in a different way, opted to rely on "domestic security service—an arguably extreme approach that is at odds with other democracies and constitutes an unprecedented privacy violation, but lays groundwork for invasive surveillance tools."[60] Israel's Security Agency was permitted to share "the name, ID number, cellphone number, internet browsing history, and every voice call and text message of confirmed COVID-19 patients."[61] The command-and-control

---

[54] Aditi Bhandari & Simon Scarr, *Reopening a Megacity*, REUTERS GRAPHICS (June 4, 2020), https://graphics.reuters.com/HEALTH-CORONAVIRUS/WUHAN/rlgpdkxzavo/index.html.
[55] Skoll *supra* note 18, at 151.
[56] Talha Burki, *China's Successful Control of COVID-19*, 20 THE LANCET 1240, 1240–1241 (2020), https://www.thelancet.com/pdfs/journals/laninf/PIIS1473-3099(20)30800-8.pdf ("As of Oct 4, 2020, China had confirmed 90,604 cases of COVID-19 and 4,739 deaths, while the USA had registered 7,382,194 cases and 209,382 deaths.").
[57] Cho, *supra* note 12, at 1.
[58] Skoll, *supra* note 18, at 151.
[59] *Id.*
[60] Tehilla S. Altshuler & Rachel A. Hershkowitz, *How Israel's COVID-19 Mass Surveillance Operation Works*, BROOKINGS (July 6, 2020), https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works/.
[61] *Id.*

approach relies on a classified database known as "The Tool," which collects cellular data about location, antenna zone, text messages, call history, and internet browsing history.[62] The program harvests metadata without consent, setting a dangerous precedent for use of overly intrusive mechanisms to combat public health crises.[63]

Finally, Singapore was the first country to deploy a national contact-tracing app.[64] On March 20, 2020, the Singapore government released a centralized application model called "TraceTogether," developed by Singapore's Government Technology Agency.[65] TraceTogether exchanges Bluetooth signals between devices in close proximity to detect other TraceTogether users.[66] The aim of the app is to quarantine people more efficiently; however, the technology is not working as the government had hoped.[67] Approximately 35% of the population has the app downloaded, but, by using Bluetooth to permit devices to exchange codes, Bluetooth must be enabled at all times which causes an immense drain on the device battery.[68] While Singapore is not employing the same mass surveillance measures that the aforementioned countries are, the TraceTogether technology has posed serious privacy concerns with respect to the government's access to the data.[69] If a user tests positive, "health officials will ask them to release their data on the app" so the government can construct a list of other people the user has been in contact with.[70] Moreover, the technology has since developed into a wearable contact tracing piece of

---

[62] *Id*.
[63] *Id*.
[64] Saira Asher, *TraceTogether: Singapore Turns to Wearable Contact-tracing Covid Tech*, BBC NEWS (July 4, 2020), https://www.bbc.com/news/technology-53146360.
[65] Singapore Government Agency Website, https://www.tracetogether.gov.sg/common/privacystatement (last visited Jan. 20, 2021).
[66] Dean Koh, *Singapore Government Launches New App for Contact Tracing to Combat Spread of COVID-19*, MOBIHEALTHNEWS (March 20, 2020), https://www.mobihealthnews.com/news/asia-pacific/singapore-government-launches-new-app-contact-tracing-combat-spread-covid-19.
[67] Asher, *supra* note 64.
[68] *Id*.
[69] Cho, *supra* note 12, at 2.
[70] *Id*.

technology.[71] This small device, referred to as a "Token," complements the existing contact-tracing app to aid in identifying people who may have been infected or who have already tested positive for the virus.[72] To use the device, a user must provide their national ID and phone number.[73] If a user tests positive, "they have to hand their device to the Ministry of Health because—unlike the app—they cannot transmit data over the internet."[74] Contact tracers then use los to identify others who may be infected.[75]

III. Privacy Threats

Subsection A explains the privacy concerns of overreach and anonymity as a result of implementing digital contact-tracing applications with a focus on the latent risk that data will be used in the future for purposes not disclosed at collection. Subsection B will then focus on the invasive nature of location tracking that are exacerbated by digital contact-tracing efforts. Subsection C will explore the concerns of voluntariness and user consent to what these apps are asking them to disclose. Finally, Subsection D examines the uncertain exit strategy that exists as nothing more but conjecture and elusive promises.

A. Overreach and Anonymity

The tradeoff between surveillance and overreach is a complicated balancing act. The graduation from traditional methods of contact-tracing to digital contact tracing has unveiled several security interests. Merely eliminating personal identification information ("PII") or only using an anonymous ID code, however, is insufficient privacy assurance.[76] Moreover, other data privacy risks include "transparency about the purpose of collecting information, the retention

[71] Asher, *supra* note 64.
[72] *Id*.
[73] *Id*.
[74] *Id*.
[75] *Id*.
[76] Hussein et al., *supra* note 33, at 3.

period, safeguarding the data, restricting access to the data, and employing anonymization techniques."[77] Intervention of contact-tracing apps raises ethical questions about just what civil liberties users are laying on the line and thus implicates careful oversight by an inclusive advisory body.[78] With specific regard to anonymity, Apple and Google, for example, have claimed that their user data "has been 'anonymized' by virtue of deidentification and decentralization."[79] Under the GDPR,[80] information is anonymized if "the information cannot be associated with a natural individual."[81] Even more, "a large range of techniques exist to re-identify individuals using seemingly anonymous information."[82]

Among other countries and including the United States, citizens have been restricted to social-distancing policies in the interest of public health. The further collection of personal information via digital contact tracing necessitates balancing the tradeoff of individual liberty interests beyond just protection of informational privacy.[83] Data protection in the broader public health framework is increasingly more crucial as countries generate and adopt different contact-tracing frameworks or applications. Effectively, a critical decision for healthcare systems using these apps is whether data is stored in central repositories or stored locally (decentralized). Because government tracking of the virus is more effective when adopting centralized models, there are additional privacy concerns as the government would have access to "citizen's location data, the 'social

[77] Todd Ehret, *Data Privacy Laws Collide with Contact Tracing Efforts; Privacy is Prevailing*, REUTERS (July 21, 2020), https://www.reuters.com/article/bc-finreg-data-privacy-contact-tracing/data-privacy-laws-collide-with-contact-tracing-efforts-privacy-is-prevailing-idUSKCN24M1NL.
[78] Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, 368 Science 1, 5 (2020).
[79] Bradford, *supra* note 42, at 6.
[80] The General Data Protection Regulation ("GDPR") is the toughest privacy and security law in the world. It imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.
[81] Bradford, *supra* note 42, at 6.
[82] *Id*.
[83] Martinez-Martin et al., *supra* note 45.

graph' of all physical contacts, and any other data the app is able to access from the phone.[84] In the United States, there is no federal privacy law so "transparency could be up to the developers' discretion" in creating these apps.

It is difficult to control overreach but if we are to invite the innovative tech industry to a partnership with the government, it must also come with internal audits and risk assessment into how individuals' data is being used. If the data is to be aggregated for the benefit of researchers and health authorities, such action exceeds the scope of what users are agreeing to by having their data collected under the assumption it is only to be used in the wake of a public health crisis. Especially in the United States, it is important to remember that "the data in question is the personal data of citizens—and in recording all of their contact interactions (and in some cases, all of their movements), it represents arguably the most personal and intimate data a government has ever sought to gather about its own citizens."[85] The importance of privacy rests on the idea that even if privacy is not a fundamental right, it is necessary to protect other fundamental rights. To "lose control of personal information is to lose control of who we are and who we can be in relation to the rest of society," and moreover, privacy is necessary as a "safeguard of freedom in the relationships between individuals and groups."[86]

In the U.S. context, questions about protecting privacy against threats of governmental surveillance implicate the Fourth Amendment, which guarantees "the right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated."[87] It should be noted that the Fourth Amendment applies only to the government and

---

[84] *Id*.
[85] Fahey & Hino, *supra* note 27, at 3.
[86] Michael McFarland, *Why We Care About Privacy*, MARKKULA CTR FOR APPLIED ETHICS (June 1, 2012), https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/; *see generally* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 5 HARV. L. REV. 93 (1890) (expressing concern with social pressure caused by excessive exposure to public scrutiny of the private affairs of individuals.).
[87] U.S. Const., amend. IV.

not private entities. Based on the surveillance programs implemented in other countries, "data aggregation for contact tracing has been and will be conducted by private entities, principally cellphone service providers and technology companies with access to location data through apps installed on users' devices.[88] With respect to data collection, as early as the 1990s, "concerns were voiced over the 'dossier' effect whereby the collection of large numbers of seemingly innocuous data points could create a combined data set with a startling amount of personal information that is easily deanonymized and attached to an individual citizen."[89] Since, the problem still remains at issue. Now, in the context of public health or under the guise of a public health crisis, there are suspicions and mistrust in both the large tech industries and the government that make progress in stopping the virus rather arduous.

B. Location Tracking

Digital contact tracing turns citizens' own smartphones into contact tracing devices making it easier to track their movements and social contacts with a heightened degree of precision.[90] It is also faster, more efficient, less labor-intensive, and less prone to human error.[91] Still, this format relies on the precise geolocation tracking and retention. When users install a contact-tracing app on a mobile device, they are prompted to enable the existing location services on that device, thus permitting the app to continuously record his or her location.[92] Typically, contact tracing requires collection of both Bluetooth and GPS data when a user comes in close proximity to another user.[93]

Given digital contact tracing is unlikely to yield its promised benefits, policymakers must "ensure that screening, testing, and isolating of affected individuals" is done before requesting or

[88] Ram & Gray, *supra* note 13, at 5.
[89] Fahey & Hino, *supra* note 27, at 3.
[90] *Id.* at 2.
[91] *Id.*
[92] Boris Segalis & Jonathan Newmark, *Road Map for a Cautious Approach to Contact Tracing*, LAW360 (April 30, 2020, 5:49 PM), https://www.law360.com/articles/1267979/road-map-for-a-cautious-approach-to-contact-tracing.
[93] *Id.*

requiring individuals sacrifice their locational and associational information.[94] Using proximity data rather than location data coupled with keeping "digital location trails" out of the government's hands could minimize the intrusiveness of gathered data and would further mitigate the privacy threats of contact tracing program.[95] To encourage trust, epidemiological surveillance programs should gather only the minimum type of data "reasonably necessary to facilitate their public health goals."[96]

In designing a contact tracing solution, "the main anchor is location data" which can be generated and collected in many ways (i.e., GPS, WIFI, Telcom Cell Towers, Bluetooth beacons).[97] Location data can be categorized in two groups: absolute location data and relative location data. First, absolute location data is "GPS location, location with respect to static WIFI access points, and Telcom cell towers," and data points are often "written in the form of geolocation coordinate pair."[98] Second, relative location data is generated from the "pairing of two Bluetooth-enabled devices," in which case there is some "reference description about the location."[99]

While large tech companies like Google and Apple promise not to track location data, any data stored on an individual's phone is by definition, "related" to an individual. The unique identifiers broadcast by the ENS can easily be linked to natural persons because "geolocation tracking systems already present on most user devices could reassociate the Bluetooth beacon identifiers with particular devices.[100] The privacy concerns of digital location tracking are further exacerbated the longer tracking data remains available to government agents. The Supreme Court

[94] Ram and Gray, *supra* note 13, at 12.
[95] *Id.* at 13.
[96] *Id.*
[97] Tang, *supra* note 14, at 6.
[98] *Id.*
[99] *Id.*
[100] Bradford, *supra* note 42, at 5.

has recognized that the nature of storing digital location tracking is "inconsistent with a central aim of the Framers."[101] While it is true that most location tracking data is obtained from individual movements in public, information "deduced from the analysis of the aggregated public data does not need to be."[102]

The Supreme Court has further rejected "any notion that technological enhancement matters to the constitutional treatment of location tracking."[103] Rather, "such surveillance in public spaces is equivalent to a 'human tail' and thus is not regulated by the Fourth Amendment."[104] In the 1967 *Katz v. United States* decision, the Court understood the Fourth Amendment insinuated that a person's "reasonable expectation of privacy" was the boundary line of protection.[105] In a post-*Katz* world, however, the notion of a privacy expectation has evolved and has broadened the physical invasion test courts used prior to deciding *Katz*.[106] Since, the Court has infused elasticity into the privacy expectation analysis as explained by Justice Harlan: "the trespass-based interpretation of the Fourth Amendment is in, the present day, bad physics, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[107]

In the Court's 2018 decision in *Carpenter v. United States*, the Court held that "the Fourth Amendment governs law enforcement access to historical cell site location gathered and stored by cellphone service providers (cellphone location data, whether in the form of cell site location or

---

[101] United States v. Di Re, 332 U.S. 581, 595 (1948).
[102] Steven Bellovin et al., *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J. L & LIBERTY 555, 622 (2014).
[103] *Id*. at 556.
[104] *Id*.
[105] Katz v. United States, 389 U.S. 347, 350 (1967).
[106] Bellovin, *supra* note 102, at 566.
[107] *Katz*, 389 U.S. at 353; *see also* Jones v. United States, 526 U.S. 227 (1999) (presenting a difficult but unavoidable choice between two competing understandings of what it meant to have a reasonable expectation of privacy under Katz.). After *Jones*, a violation of the Fourth Amendment can be established with a showing that law enforcement attempted to gather information either by an unauthorized physical intrusion of a protected space or by invading reasonable expectations of privacy.

GPS tracking), appears to be a centerpiece of tracing and proximity surveillance proposals because these devices are so often with their users."[108] Moreover, this holding established that individuals have the right to expect that "the whole of their physical movements" will remain private.[109] Location data from smartphones and cellphones "provide an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.[110] Even though this decision was applicable only to government actors, the case's particular holding on the sensitivity of location data will likely have wide-ranging implications for private companies' privacy programs. The Court further explained that their holding with regards to cell site location information ("CLSI") was a "narrow one" and in their opinion, the Court planned to "tread carefully in such cases" so as not to "embarrass the future."[111] The crux of the Court's reasoning was that "location tracking reveals a host of intimate details about private associations and activities."[112] Contact tracing applications, location monitoring, and other epidemiological surveillance programs that prove to be robust enough to document disease progression using aggregate data will trigger the concerns observed in *Carpenter*.[113]

Although defended on grounds of urgent need to contend with the present health crises, the variation of digital contact tracing efforts raise significant cause for concern given their potential for abuse. Despite potential public health benefits, it is not entirely clear that digital contact tracing can achieve its aim of curbing the virus without imposing disproportionate privacy harms. It is not without acknowledging that the explosive growth of COVID-19 in the United States alone

[108] Carpenter v. United States, 138 U.S. 2206, 2267 (2018) (Gorsuch, J., dissenting); *see also* Riley v. California, 573 U.S. 373, 395 (2014) ("It is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from mundane to intimate.").
[109] *Carpenter*, 138 U.S. at 2217.
[110] *Id.*
[111] *Id.*
[112] *Id.* at 2217–18.
[113] Ram & Gray, *supra* note 13, at 8.

"crippled American life and the economy," thus triggering an increased interest in "harnessing the power of [technology] to track, predict, and control the pandemic."[114] Despite this desperation for a quick fix, policy makers in partnership with technology developers must weigh the comparative advantages of location tracking against a more traditional means of controlling a pandemic, taking into account serious threats to privacy, metrics that will determine success in implementing digital contact-tracing models, and set plans for sunsetting the data at the end of the public health crisis.[115]

C. Voluntariness and Consent

For contact tracing apps and exposure notification systems to work, it is critical that enough people trust the app to install it and provide highly personal information to help accurately track the spread of the virus. Implementation of the app "must have a higher 'transmission rate' than the virus itself for it to be effective.[116] Providing stronger privacy protection would likely encourage voluntary adoption, a choice made by a user's free will rather than through coercion coerced.[117] For contact-tracing apps to be truly voluntary, the following must be the user's free choice: the decision to carry a smartphone, the decision to download the app, the decision to leave the app operating on the device at all times, the decision to react to its alerts, and the decision to share the contact logs when tested positive.[118] Heightened public anxiety surrounding the privacy concerns ultimately impedes voluntariness, though. If not enough of the population downloads a proposed contact tracing app, the effectiveness of said app is squandered. On the other hand, if the app's use is mandated, this is equally problematic as it amounts to indirect coercion. An Oxford University study suggested "at least 60% of a country's population would need to use an app" to

[114] *Id.* at 2.
[115] *Id.* at 4.
[116] Cho, *supra* note 12, at 8.
[117] *Id.*
[118] *Id.*

stop the spread of the virus.[119] In the United States, a survey by the Washington Post-University of Maryland found only about half of Americans who own smartphones would be willing to use the Google/Apple ENS framework.[120]

Voluntariness blends with the element of consent as well. While many people are willing to consent to health systems to use their personal data to track exposure, "consent is not the optimal basis for public authorities. Consent given to public authorities is generally not considered to be given freely due to the power or potential power of public agencies to compel compliance."[121] In the U.S., nearly three in five people are not willing to download and use a contact-tracing app due to the mistrust of tech companies and their willingness (or lack thereof) to safeguard privacy.[122] If Google/Apple begins partnering with governments, requiring explicit consent supports autonomy over users' personal information and further limits what data is controlled and how long it is retained.[123] Nonconsensual tracking by law enforcement increases the risks that a government agency will abuse their authority by using public health data beyond the scope of its intended purpose. This would be detrimental to the trust and relationship between the government and the public.

D. Exit Strategy

It is imperative that a well designed contact-tracing solution, designed to combat a viral outbreak, be paired with strict sunsetting provisions. While the implementation of digitized contact-tracing applications is beneficial for the efficiency of tracking mass groups of individuals, once a tool like this is operational, it is tempting to store information and use it to develop strategies

[119] Garner, *supra* note 26.
[120] *Id.*
[121] Bradford, *supra* note 42, at 12.
[122] *Id.* at 22.
[123] *Id.* at 13.

for future infectious diseases. Implementing these technologies and designing them with the future in mind will likely lead to changes in our laws governing civil rights. Despite this, "justice and autonomy in patient-care . . . should not be forsaken," even amidst a pandemic.[124] To that end, healthcare interventions by tech developers must be transparent about "the roadmap to scaling" and implementing digital-contact tracing efforts when it requires such a "comprehensive socio-political buy-in."[125] The suspicions circulating about contact-tracing efforts and applications could have "a cost measured in lives."[126] If there is insufficient participation in tracking, the ongoing collection efforts suffer. Such suspicious are rooted in the ambiguities about whether or not there is a plan to sunset the data individuals are contributing. Minus assurances of privacy protection measures by tech developers creating decentralized models, there has not been a clearly defined exit strategy for when the pandemic ends.

IV. Current Privacy Law: HIV/AIDS Comparison and Legal Framework

A. HIV Contact-Tracing

In the infectious disease context, the justification for contact tracing is that in "requiring scientific evidence that the person actually has an infectious condition, that circumstances exist whereby the infection can be communicated," then that "measure would be effective in eliminating or reducing the risk of contagion."[127] Traditional contact tracing efforts trace back to sixteenth century Europe when even then it was a governmental responsibility for public health authorities.[128] At the turn of the twentieth century, the HIV/AIDS epidemic presented new challenges for public health officials. From the epidemic's inception, patient-confidentiality in the

[124] Martinez-Martin et al., *supra* note 45.
[125] *Id*.
[126] Fahey & Hino, *supra* note 27, at 2.
[127] Matthew L. Levine, *Contact Tracing for HIV Infection: A Plea for Privacy*, 20 COLUM. HUM. RTS. L. REV. 157, 164 (1988).
[128] Lawrence Gostin and James Hodge, *Piercing the Veil of Secrecy in HIV/ AIDS and Other STDs: Theories of Privacy and Disclosure in Partner Notification*, 5 (1998).

context of contact tracing resurfaced and met a new level of intensity. At this time, however, the public health response focused primarily on individual responsibility. In the context, of HIV, health departments interviewed infected patients ("index cases") who would voluntarily disclose names of past and present sexual partners who were then traced in order to be notified of their potential exposure.[129] Because of prevailing social mores that keep sexually transmitted diseases (STDs) out of the eyeline of public consciousness, the spread of STDs typically do not receive effective intervention.[130] Secrecy and individual privacy were a "prevailing social construct of public health,"[131] and with regard to AIDS, the disease fostered "ominous fantasies . . . that is a marker of both individual and social vulnerabilities."[132] To "pierce the veil of secrecy" surrounding these diseases, one of the earliest strategies for STD prevention was "sexual contact-tracing" in the form of two models: patient referral and provider referral.[133] The use of contact-tracing per these arrangements are limited. Because of the "deep intrusion into private matters that tracing involves and the great stigma that is associated with HIV infection," contact-tracing without strict confidentiality laws disincentivize transparency about having the condition.[134] In 1987, the Centers for Disease Control and Prevention (CDC) set guidelines regarding HIV contact-tracing, stating, "If [people infected with HIV] are unwilling to notify their partners . . . physicians or health department personnel should use confidential procedures to assure that the partners are notified."[135] The most pressing issue involved in this contact tracing scheme is the "invasion of the constitutional right of informational privacy and the potentially discouraging effect on risk-

[129] *Id*.
[130] *Id*. at 2.
[131] *Id*. at 3.
[132] *Id*.
[133] *Id*.
[134] Levine, *supra* note 127, at 168–69.
[135] Michael Walder, *Contact Tracing for HIV Infection*, 296 BRITISH MED. J. 1420, 1421 (1988).

reduction behavior resulting from contact tracing."[136] The unwarranted and unprotected disclosure of HIV-related information, while important to curb the spread and protect lives of those who may be at risk, raises an expectation for privacy as it implicates one's constitutional right to keep certain personal information private.[137]

In the modern context, many have expressed privacy concerns regarding digital contact tracing solutions and the loss of agency. Since the first reported AIDS case, sociologists interviewed patients and documented environmental factors that would later help the CDC determine the cause of the immunodeficiency—a virus, and not chemicals or recreational drug use as initially believed.[138] The development of trust between patients and sociologists was crucial in acquiring this information. Trust and participation of the community are imperative to effective, large-scale contact tracing efforts that garner qualitative data to understand how a virus spreads between contacts and risk factors that make others more susceptible.[139] Naturally, digital contact tracing apps make this more difficult, especially those that employ a centralized model or use location tracking. Without patients' trust and consent to share data, progress in stopping the spread of COVID-19 could face heavy consequences of relying too much on technology as the solution. In the U.S., especially with such limited trust in leadership and the current administration, asking the public to put trust in large tech companies like Apple and Google is a tall order.

V. Solution/Conclusion

As society progresses and as the intuitive technology development sector continues to flourish, it is inevitable that privacy-aware solutions be designed and integrated to fulfill the objectives of contact-tracing in a digital context in the face of a global pandemic. The main problem facing these

[136] Levine, *supra* note 127, at 183.
[137] *Id.*
[138] Dragana Kaurin, *The Dangers of Digital Contact Tracing: Lessons from the HIV Pandemic*, at 64 (Aug. 8, 2020).
[139] *Id.*

new solutions is a mass consensus to trust technology developers and their role in the scope of contact tracing. One thing is clear, mass surveillance models like those deployed in China, South Korea, Israel, and Singapore will be entirely unworkable in the United States. The United States is pressed to adopt some form of a national contact-tracing framework as well as enhanced testing strategies to balance the needs of public health while respecting individual liberties. In evaluating the differences between decentralized and centralized models of digital contact tracing apps, a decentralized framework is less threatening to the various privacy risks to which digital contact-tracing opens the door. The Apple/Google ENS proposal and partnership with public health officials is a good start, but utility of the framework will depend on reliability of diagnosis information and the availability of COVID-19 testing. Only with these complementary capacities can exposure notification and contact-tracing manifest further as a proportionate response to COVID-19 management and moreover justifies a level of intrusion on individuals' privacy rights. Additionally, there should be "incentive mechanisms" built into the applications beyond opting-in and opting-out.[140] Because user participation is so crucial to the effectiveness of these applications, incentivizing such participation by utilizing an app that requires explicit consent, encourages voluntariness, and strictly limits what data is collected to only that which is entirely necessary and preventing use of any surveillance tool for either political or economic purposes is crucial. Government authorities must monitor their contact tracing system to prevent against function creep,[141] such that the data is not kept after the public health crisis ceases. Finally, privacy requirement in the form of legislation would be beneficial so a user can disclose necessary information to public health officials without facing social embarrassment or discrimination. Such

[140] Tang, *supra* note 14 at 17.
[141] Function creep occurs when information is used for a purpose other than its specified purpose.

a legal instrument could establish accountability mechanisms, ensuring private use of the data is appropriately responsive to public concerns and democratic principles.[142]

Effective digital contact tracing can be a highly effective step towards containing future outbreaks. There is a variety of digital technologies unveiling around the world to help curb the spread of the virus, but that simultaneously harm privacy.[143] Some of the frameworks, like the Apple Google ENS proposal, have been designed with privacy and security in mind.[144] The decentralized architecture does not report information about contacts or connections a user's device has made to a central server but rather stores such data on each individual's device.[145] This framework ensures protection of users' privacy by allowing users full control over the ENS system,[146] by not sharing geographic location with the government, and by preserving users' identities if they test positive.[147] However, security concerns still remain, leaving users vulnerable to risk of overreach and other privacy violations.[148] Further protections should be afforded to users by ensuring that the data being analyzed is accurate and that there is heightened transparency from the government and tech developers. The success of any digital contact tracing app depends fully on trust, reliability, and widespread use. In order to be considered as an operative public-health tool for future pandemics, safeguarding privacy must be the first step in devising contact-tracing solutions.[149] Moving forward, there are three critical privacy risks that must be mitigated:

---

[142] Bradford, *supra* note 42, at 21.
[143] Simon Chandler, *Coronavirus Contact-Tracing Apps Miss The Point About Privacy*, FORBES (May 4, 2020), https://www.forbes.com/sites/simonchandler/2020/05/04/coronavirus-contact-tracing-apps-miss-the-point-about-privacy/?sh=cd4503a39c46.
[144] Ashkan Soltani et al., *Contact-Tracing Apps are Not a Solution to the COVID-19 Crisis*, BROOKINGS (April 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.
[145] *Id.*
[146] It is up to the individual user of each device when to turn the app on or off.
[147] Ashkan Soltani et al., *supra* note 144.
[148] *Id.*
[149] Aaqib Bashir Dar et al., *Applicability of Mobile Contact Tracing in Fighting Pandemic (COVID-19): Issues, Challenges, and Solutions*, 38 COMPUT. SCI. REV. 2, 4 (2020).

indefinite storage of COVID-19 personal data; repurposing COVID-19 data for uses unrelated to managing the public health crisis; and unauthorized access to COVID-10 personal data by any entity without legitimate need related to the current public health crisis.[150] To respond to these risks, digital contact tracing solutions must be designed to make sensible trade-offs between competing priorities of managing the public health crisis and protecting privacy. Beyond the design of the apps themselves, the U.S. needs a baseline federal privacy law to establish clear and enforceable privacy rules that protects users personal information, especially in times of crisis.

[150] Jane Bambauer & Brian Ray, *Covid-19 Apps are Terrible—They Didn't Have to Be*, 7 THE DIGITAL SOCIAL CONTRACT (November 2020), https://www.lawfareblog.com/covid-19-apps-are-terrible-they-didnt-have-be.