RUTGERS JOURNAL OF LAW & PUBLIC POLICY

VOLUME 19 FALL 2021 ISSUE 1

About the Rutgers Journal of Law & Public Policy

The *Rutgers Journal of Law and Public Policy* (ISSN 1934-3736) is published two times per year by students of the Rutgers School of Law – Camden, located at 217 North Fifth Street, Camden, NJ 08102. The views expressed in the *Rutgers Journal of Law & Public Policy* are those of the authors and not necessarily of the *Rutgers Journal of Law & Public Policy* or the Rutgers School of Law – Camden.

Form: Citations conform to *The Bluebook: A Uniform System of Citation* (21st ed. 2021). Please cite the *Rutgers Journal of Law & Public Policy* as 19 RUTGERS J.L. & PUB. POL'Y __ (2021).

Manuscripts: The *Rutgers Journal of Law & Public Policy* seeks to publish articles making original contributions in the field of public policy. The *Journal* accepts both articles and compelling essays for publication that are related to the expansive topic of public policy. Manuscripts must contain an abstract describing the article or essay which will be edited and used for publication on the website and in CD-ROM format. The *Journal* welcomes submissions from legal scholars, academics, policy makers, practitioners, lawyers, judges and social scientists.

Electronic submissions are encouraged. Submissions by email and attachment should be directed to submissions@rutgerspolicyjournal.org.

Paper or disk submissions should be directed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102.

Subscriptions: Subscription requests should be mailed to *Rutgers Journal of Law & Public Policy*, Rutgers University School of Law – Camden, 217 North Fifth Street, Camden, New Jersey 08102, or emailed to info@rutgerspolicyjournal.org.

Internet Address: The *Rutgers Journal of Law & Public Policy* website is located at http://www.rutgerspolicyjournal.org.

PROFESSORS OF LAW EMERITI

FRANK ASKIN, B.A., J.D., *Distinguished Professor of Law Emeritus, Robert E. Knowlton Scholar, and Director of the Constitutional Rights Clinic*
PAUL AXEL-LUTE, B.A., M.L.S., *Deputy Director of the Law Library Emeritus*
CYNTHIA A. BLUM, B.A., J.D., *Professor of Law Emerita*
A HAYS BUTLER, B.A., J.D., M.S. (LIS), *Law Librarian Emeritus*
NORMAN L. CANTOR, A.B., J.D., *Professor of Law Emeritus*
EDWARD E. CHASE, B.A., J.D., *Professor of Law Emeritus*
ROGER S. CLARK, B.A., LL.B., LL.M., J.S.D., L.L.D., *Board of Governors Professor and Distinguished Professor of Law Emeritus*
RUSSELL M. COOMBS, B.A., J.D., *Professor of Law Emeritus*
LUCY COX, B.A., M.S., Ph.D., M.L.S., *International and Foreign Law Librarian Emerita*
ANNE V. DALESANDRO, A.B., M.L.S., J.D., *Law Library Director Emerita and Professor of Law Emerita*
JOHN H. DAVIES, B.S., LL.B., LL.M., *Professor of Law Emeritus*
STUART L. DEUTSCH, B.A., J.D., LL.M., *University Professor and Willard Heckel Scholar*
JACK FEINSTEIN, B.A., J.D., *Clinical Professor of Law Emeritus*
GEORGE GINSBURGS, B.A., M.A., Ph.D., *Distinguished Professor of Law Emeritus*
ARNO LIIVAK, B.A., M.L.S., J.D., *Professor of Law Emeritus*
JONATHAN MALLAMUD, A.B., J.D., *Professor of Law Emeritus*
CRAIG N. OREN, A.B., J.D., *Professor of Law Emeritus*
JAMES GRAY POPE, A.B., J.D., Ph.D., *Distinguished Professor of Law and Sidney Reitman Scholar*
PATRICK J. RYAN, B.A., M.A., J.D., LL.M., J.S.D., *Associate Professor of Law Emeritus*
CAROL ROEHRENBECK, B.A., M.L.S., J.D., *Professor of Law and Director of the Law Library Emerita*
RAND E. ROSENBLATT, B.A., M.Sc., J.D., *Professor of Law Emeritus*
DIANA SCLAR, B.A., J.D., *Professor of Law*
PETER SIMMONS, A.B., LL.B., *University Professor Emeritus, John M. Payne Scholar*
RICHARD G. SINGER, B.A., J.D., LL.M., J.S.D., *Distinguished Professor of Law Emeritus*
E. HUNTER TAYLOR, B.A., LL.B., LL.M., *Professor of Law Emeritus*
PAUL L. TRACTENBERG, B.A., J.D. *Board of Governors Distinguished Service Professor and Professor of Law*
ROBERT M.WASHBURN, A.B., J.D., LL.M, *Professor of Law Emeritus*
ROBERT F. WILLIAMS, B.A., J.D., LL.M., *Distinguished Professor of Law Emeritus*

FACULTY OF LAW

AARON ARI AFILALO, A.B., J.D., LL.M., *Professor of Law*
CHARLES AUFFANT, B.A., J.D., *Clinical Professor of Law*
SAHAR AZIZ, B.SC., M.A., J.D., *Professor of Law*
CARLOS A. BALL, B.A., J.D., LL.M., *Distinguished Professor of Law*
BERNARD W. BELL, B.A., J.D., *Professor of Law*
VERA BERGELSON, J.D., Ph.D., *Distinguished Professor of Law*
AMY BITTERMAN, B.A., J.D., *Assistant Clinical Professor of Law*
ELISE BODDIE, B.A., M.P.P., J.D., *Professor of Law*
LINDA S. BOSNIAK, A.B., M.A., J.D., Ph.D., *Distinguished Professor of Law*
ESTHER CANTY-BARNES, B.A., J.D., *Clinical Professor of Law*
MICHAEL A. CARRIER, B.A., J.D., *Distinguished Professor of Law*

STAFF AND ADMINISTRATION

ELSPETH ABEL
ELIZABETH ACEVADO
ANGELICA AGUIRRE
LISA ALSTON
REBECCA BAEHR
JEFFREY BALOG
JOANN BREA
PATRICIA BROWN
LORETTA BURR
ANGELA CAMPIONE
VIRGINIA CAPUTO
MAYRA CARABALLO
DEBORAH CARR
BERNADETTE CARTER
ROSELENE CORREIA
GINA DAVILA
CLIFFORD DAWKINS
FRANNIE DESIMONE
TIMOTHY DIVITO
CHRISTINE DOUGHERTY
RHASHEDA DOUGLAS
GRACE DUFFIN
SUSAN FEATHERS
ANDREW FINN
JILL FRIEDMAN
SONDRA FURCAJG
LINDA GARBACCIO
ROBERTA GEDDIS
TAI GEDEON
ELAINE GIORDANO
ARBANA GJOCA
KATRINA HALL
JASON HERNANDEZ
DENISE HIGGINS
DAVID HORAN
CASSANDRA HUNTER
YVENA HYPOLITE
WANDA JAMES
HABIBAH JOHNSON
DENISE JOHNSON-STEINERT
MELISSA JORDAN
DEBORAH LEAK
ARLENE LENTINI
CASSANDRA LESTER-KEY
MARGARET MCCARTHY
PAM MERTSOCK-WOLFE
ELIZABETH MOORE
JOSEPHINE NAGLE
NATHANIEL NAKAO
EDGAR OTIENO
LENORE PEARSON
MARIE PEEKE
MILDRED PEREZ
CHRISTOPHER PHILLIPS
SARAH K. REGINA
NANCY RUBERT
THOMAS RYAN
DANIEL SANDERS
CAROL SHANER
CHRISTOPHER SLATER
STAN SNIECIKOWSKI
DONNA TAGLIAFERRO
MARTHA TAYLOR
WENDI L. TAYLOR
AMY TIMKO
ROBIN TODD
GWEN TOLBERT
CHERYL TURK
MARVIN VELASCO
REBECCA VERONA
ELIZABETH YEAGER
ANITA WALTON
CLAIRE WHITE
NEIL WISE

RUTGERS

JOURNAL OF LAW & PUBLIC POLICY

VOLUME 19 FALL 2021 ISSUE 1

Current Issues in Public Policy

ISSN 1934-3736

CONTACT TRACING: WHERE WE WERE, WHERE WE ARE, WHERE WE ARE GOING. THE INFLUENCE "PRIVACY BY DESIGN" HAS HAD ON CONTACT TRACING APPS AND THE LASTING IMPRESSION IT WILL HAVE WELL AFTER THE PANDEMIC IS OVER

Taylor Farrow

I. INTRODUCTION

As COVID-19 has spread globally, the underlying conflict between personal privacy rights and public well-being rages on, with no clear solution to either in sight.[1] With the intention of managing the spread of the virus, "tech companies and governments have both sought to come up with effective yet socially distant ways to keep close tabs on people's health status and movements."[2] The presented solution, digital contact tracing, uses technology to collect vital but sensitive health and location information, which has presented issues that have not yet been featured in the long-running privacy debate.[3] According to Kate Goodloe, Director of Policy at BSA: The Software Alliance, the pandemic has highlighted the "need to use data in important ways, but also the importance of getting it right when it comes to the type of privacy and security safeguards that need to be placed on different uses of data."[4]

The most looming question is "whether companies should have some type of exemption or liability shield for collecting, using or sharing data in certain circumstances" or in other words, "whether data limitations should be eased for some purposes."[5] The pandemic may welcome more sympathy to loosening restrictions on the uses of personal data; however, this is not the solution that will generate the public trust necessary for digital contact tracing methods to be effective.[6] According to Jessica Rich, former Director of Consumer Protection at the Federal Trade Commission and a longtime manager of the FTC's privacy program, the public does not trust that their personal health and location data that contact tracing apps collect will be protected once in the hands of either the government or Big Tech companies.[7] Rich goes on to indicate that this lack of trust is supported by past misuse and abuse of the public's personal data that the

---

[1] Allison Grande, *How COVID-19 Is Set to Reshape Federal Privacy Law Debate*, LAW360 (May 7, 2020, 12:43 PM), https://www.law360.com/articles/1267255.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] Grande, *supra* note 1.
[6] *See id.*
[7] Jessica Rich, *How our Outdated Privacy Laws Doomed Contact-Tracing Apps*, BROOKINGS: TECHTANK (Jan. 28, 2021), https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/.

government and Big Tech companies have collected, used, and stored.[8] Without public trust and assurances of privacy protections, digital contact tracing will not be an effective tool in stopping the spread of COVID-19 or even future outbreaks.

If digital contact tracing is to be effective against the spread of COVID-19, there needs to be a balance between efficiently using personal data to stop the pandemic and how individuals' privacy can be protected in the process.[9] Without a baseline federal data protection law to protect the sensitive data obtained through these apps, there must be reliance on Big Tech companies to incorporate strategies that ensure privacy protections throughout the development of contact tracing technology.[10]

"Privacy by Design" is a strategy that encompasses privacy protecting principles that are aimed at instilling trust and assurance in the use of new and innovative technology.[11] Digital contact tracing does not need to come at the cost of the public's right to privacy if contact tracing technology is deliberately and systematically built with privacy protections at its core.[12] Digital contact tracing developed with the principles of "Privacy by Design" can be used to combat the spread of COVID-19 without jeopardizing individuals' right to privacy.[13]

---

[8] *Id.*

[9] *See generally* Grande, *supra* note 1; *see also* Samuel Volkin, *Digital Contact Tracing Poses Ethical Challenges*, JOHNS HOPKINS: HUB (May 26, 2020), https://hub.jhu.edu/2020/05/26/digital-contact-tracing-ethics/ ("Respecting privacy is a core ethical principal and is actually driving the conversation of whether digital contact tracing should be used in the United States.").

[10] Rich, *supra* note 7.

[11] *See generally* ANN CAVOUKIAN, INFO. & PRIV. COMM'R ONT., PRIVACY BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (2011), https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

[12] *Id.*; *see generally* Ummey Kulsum & Jasmine Khan, *Data Privacy as an Indispensable Asset- Its Significance and Way Forward*, INDIAN SOC'Y FOR LEGAL RSCH. (Sept. 23, 2020), https://indiansocietyforlegalresearch.in/2020/09/23/data-privacy-as-an-indispensable-asset-its-significance-and-way-forward/.

[13] *See* Jeremy Kirk, *Building Privacy-Centered Contact Tracing Apps*, BANK INFO SEC. (Sept. 2, 2020), https://www.bankinfosecurity.com/interviews/building-privacy-centered-contract-tracing-apps-i-4756.

Bluetooth and GPS are the two widely available digital contact tracing technologies currently being used in the fight against COVID-19.[14] Through Bluetooth technology, Apple and Google have developed the Exposure Notification system ("ENS") that will notify users of potential COVID-19 exposure while protecting one's privacy.[15] ENS has been built with privacy at its core in a deliberate and systematic way that puts the user in control.[16] The "Privacy by Design" principles have been assimilated into the Exposure Notification system to provide the broadest possible assistance in stopping the spread of COVID-19 while maintaining individuals' privacy.[17] Access to the ENS technology will only be granted to public health authorities who developed an app that meets specific standards for privacy, security, and data control.[18] Apple and Google did release an app, the EN express, that will allow public health authorities to utilize ENS without the hassle of developing their own compatible app.[19]

Although there still seems be a slow willingness to adopt apps that utilize the Exposure Notification system, the incorporation of the "Privacy by Design" principles into this technology is the first step in generating public trust so that these apps can be effective against the spread of COVID-19 and future outbreaks.[20] There is evidence that even low adoption rates can have an impact in stopping the spread of COVID-19.[21] Additionally, states that have recently released the EN

---

[14] Robert Cattanach & Nur Ibrahim, *Contact Tracing: Strategies and Issues for Balancing Public Health Demands and Privacy Concerns*, 35 ANTITRUST 18, 20 (2020).

[15] Albert Gidari, *Privacy and New Google-Apple COVID-19 Tracing Technology: Q&A with Sharon Driscoll*, STAN. L. SCH.: LEGAL AGGREGATE (May 7, 2020), https://law.stanford.edu/2020/05/07/privacy-and-new-google-apple-covid-19-tracing-technology/.

[16] *Id.*; *see generally* APPLE & GOOGLE, *Exposure Notifications, Frequently Asked Questions*, APPLE GOOGLE (Sept. 2020), https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf.

[17] Gidari, *supra* note 15.

[18] APPLE & GOOGLE, *supra* note 16.

[19] *Exposure Notification Express Overview*, GOOGLE, https://developers.google.com/android/exposure-notifications/en-express (last updated Nov. 9, 2020).

[20] *See generally* Grande, *supra* note 1.

[21] Nalike Vasudevan & Abhilash Panthagani, *Why Exposure Notification Technology Should Still be on Your Agenda for Spring 2021*, EAB (Jan. 12,

Express app and are utilizing the app's ability to send push notifications have experienced higher adoption rates.[22]

It is easy to come to the conclusion that digital contact tracing efforts failed especially when the Exposure Notification system, that was built deliberately and systematically with privacy protections from end-to-end, was unable to reach substantial adoption rates.[23] However, this technology will have an impact on preventing future outbreaks, on future privacy protection laws and future technology that will rely on public trust to be effective. This is already the case as vaccine apps are being developed, which will allow individuals to quickly provide vaccination verification right on their smartphones.[24] Vaccine app developers are being encouraged to adopt privacy protections similar to those found in the ENS so that the public will be more inclined to use these apps.[25] Without a comprehensive federal privacy law and patchy state privacy laws, Big Tech companies must instill privacy protections in these technological efforts aimed at assisting the current pandemic and the publics overall well-being.

Part II will discuss the long-standing reliance on traditional contact tracing as a method to stop the spread of infectious diseases. This section will evaluate what contact tracing is, the privacy concerns it has caused during previous outbreaks, specifically the HIV epidemic, and how it is dependent upon public trust in order to be effective.

Part III will focus on COVID-19 and how it has and continues to impact the United States. It will address how the virus spreads and that traditional contact tracing has not been enough to sufficiently slow the spread.

Part IV provides an overview of digital contact tracing and how other countries are using it. This section will review the states and

---

2021), https://eab.com/insights/expert-insight/it/exposure-notification-technology-spring-2021/.

[22] Kif Leswing, *California Says 10% of State has Opted into Coronavirus Exposure App,* CNBC (Dec. 13, 2020, 1:06 PM) https://www.cnbc.com/2020/12/12/ca-notify-coronavirus-app-gets-4-million-activations-in-first-day.html.

[23] Rich, *supra* note 7.

[24] Ron Raether et al., *Data Compliance Issues for Companies Making, Using Vaccine Apps,* LAW360: EXPERT ANALYSIS (Feb. 10, 2021), https://www.law360.com/articles/1352956/data-compliance-issues-for-cos-making-using-vaccine-apps.

[25] *Id.*

countries who opted to make use of contact tracing apps voluntary and the effective adoption rate needed to impact the spread of COVID-19.

Part V reviews the underlying privacy concerns that have contributed to Americans' unwillingness to participate in sharing the necessary personal information and data that contact tracing apps need to be effective. The concerns that will be addressed include lack of trust that information will remain private, discomfort in who will have access to this personal data, misuse of the information that will be collected, and the impact on vulnerable communities.

Part VI explains the seven principles of "Privacy by Design." This section will provide a brief summary of the principles as presented by Ann Cavoukian, Ontario's Information & Privacy Commissioner.[26]

Part VII introduces the Exposure Notification system and how it works. This section will outline the privacy protections within the Exposure Notification system and how these safeguards satisfy the principles of "Privacy by Design."

Part VIII discusses how contact tracing apps operating with the ENS are still experiencing minimal adoption rates, despite the "Privacy by Design" supported safeguards. It will highlight the positive impact ENS apps have had on college campuses and how college students have a better understanding of the apps, thus trusting the privacy protections the apps are equipped with. This section will show that while the privacy protections are crucial, other factors are contributing to adoption rates remaining low, such as states only just recently utilizing the EN Express app and the push notification option.

Part IX will conclude with emphasizing that overlooking infringement on our right to privacy during the pandemic could negatively impact our ability to resist future diminishment of privacy protection. "Privacy by Design" is a crucial step for Big Tech companies to take when developing contact tracing apps but must be followed up by federal and local government efforts to actually put an end to the COVID-19 pandemic. Additionally, this section will address vaccine apps and how the ENS inclusion of "Privacy by Design" principles should be standard when developing these apps as well.

[26] CAVOUKIAN, *supra* note 10.

II. CONTACT TRACING HISTORY

Controlling the spread of novel and often deadly diseases has been a reoccurring problem the human race has dealt with for centuries.[27] Although the problematic disease has differed throughout time, the methods used to locate those infected and stop the spread has remained consistent.[28] Even though contact tracing has been an effective tool for past public health emergencies, the process has always required individuals to disclose sensitive and private information.[29] Essentially, effective contact tracing has, by its nature, posed a risk to the right to privacy.[30]

Contact tracing is a century old mechanism that has been used to combat the spread of HIV, syphilis, Yellow Fever and even the bubonic plague.[31] This method has been an "essential part of preventing subsequent infections during an epidemic," according to Associate Vice President for Research and Innovation at Virginia Tech, Lisa M. Lee, PhD.[32] Contact tracing is especially forthcoming because of the necessary time it takes to develop a vaccine and the immediate need to stop the spread of the infectious disease.[33] Contact tracing is "characteristically a governmental responsibility undertaken by public health authorities."[34] The World Health Organization defines contact tracing as a "monitoring process in which an infected person identifies

---

[27] *See generally* Samuel Cohn & Mona O'Brien, *Contact Tracing: How it was Used 500 Years Ago to Control the Bubonic Plague*, CONVERSATION (June 3, 2020, 7:06 AM), https://theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248; *see generally* Lawrence O. Gostin et al., *Piercing the Veil of Secrecy in HIV/AIDS and Other Sexually Transmitted Diseases: Theories of Privacy and Disclosure in Partner Notification*, 5 DUKE J. GENDER L. & POL'Y 9, 14 (1998).

[28] *See generally* Gostin et al., *supra* note 27.

[29] *Id.* at 13.

[30] *Id.*

[31] Cohn & O'Brien, *supra* note 27; *see generally* Sean Bland, *Reflections on the History of Contact Tracing*, O'NEILL INST. NAT'L & GLOB. HEALTH L. (July 13, 2020), https://oneill.law.georgetown.edu/reflections-on-the-history-of-contact-tracing/.

[32] Shawn Radcliffe, *How Contact Tracing Can Help Stop COVID-19*, HEALTHLINE (May 4, 2020), https://www.healthline.com/health-news/everything-to-know-about-contact-tracing (last visited Nov. 16, 2021, 2:38 PM).

[33] *Id.*

[34] Gostin et al., *supra* note 27, at 14.

all other individuals with whom they have been in contact."[35] Traditionally, contact tracing is performed manually by either public health departments or a patient's own doctors.[36] A trained public healthcare professional interviews an infected person in order to gather information about where that person has been and who she has been in contact with.[37] These contacts are then located and notified of their potential exposure to the infection.[38] The process is then continued until all contacts are notified and informed of the potential exposure to infection, testing information, and risk reduction.[39]

Although it is necessarily invasive and labor intensive, manual contact tracing provides a human approach to addressing the spread of infectious diseases.[40] Trained professionals will attempt to address and understand any concerns an infected person is facing.[41] These professionals will do some analysis with the infected person to determine who she remembers being in contact with during the period of contagiousness.[42] This process is also limited to what the infected person is willing to share.[43]

Contact tracing has historically been useful in outbreaks of sexually transmitted diseases.[44] The syphilis epidemic of the sixteenth century in Europe illuminates the development and origin of contact

---

[35] Natalie Ram et al., *Mass Surveillance in the Age of COVID-19*, 7 J. L. BIOSCIENCE 1, 3 (2020).

[36] *Covid Contact Tracing Apps Are a Complicated Mess: What You Need to Know*, PRIV. INT'L (May 19, 2020), https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know/; *see generally* Nancy E. Kass & Andrea Carlson Gielen, *ARTICLE: The Ethics of Contact Tracing Programs and Their Implications for Women*, 5 DUKE J. GENDER L. & POL'Y 89, 90 (1998).

[37] Radcliffe, *supra* note 32; *see* RJ Vogt, *How Virus Surveillance and Civil Liberties Could Collide*, LAW360 (Apr. 26, 2020, 8:02 PM), https://www.law360.com/articles/1267269/how-virus-surveillance-and-civil-liberties-could-collide.

[38] Gostin et al., *supra* note 27, at 26-27; *see* Kass & Gielen, *supra* note 36.

[39] Kass & Gielen, *supra* note 36, at 91.

[40] *See* PRIV. INT'L, *supra* note 36; *see generally* Christine Lehmann, *Privacy Concerns Hindering Digital Tracing*, WEBMD (Sept. 25, 2020), https://www.webmd.com/lung/news/20200928/privacy-concerns-hindering-digital-contact-tracing.

[41] *See* PRIV. INT'L, *supra* note 36.

[42] *Id.*

[43] *Id.*

[44] Gostin et al., *supra* note 27, at 11-12.

tracing.[45] Thought to have come from the New World, syphilis quickly spread after the French ruler, Charles VIII, dispersed the multinational mercenary army.[46] Eventually syphilis was recognized as a sexually transmitted disease that could be controlled by regulating the source of infection.[47] These early methods of source identification included banishment from the community, quarantining those infected in special hospitals, or simply prohibiting the infected from entering public areas or associating with certain people.[48] Contact tracing was again relied on once the human immunodeficiency virus ("HIV") epidemic presented new challenges for public health officials.[49]

The traditional contact tracing process can be an effective tool to stop the spread of an outbreak, but it is not without its limitations.[50] The process is often encumbered because of inadequate and limited access to testing, which can result in false positives and unnecessary contact tracing.[51] It is additionally obstructed when fears and concerns about disclosing information override one's desire to assist in stopping the spread of an outbreak.[52] During the HIV epidemic, the societal response was fear and stigmatization of those infected, which had an impeding effect on one's willingness to participate in contact tracing.[53] Although public health departments are expected to be non-judgmental with the sole focus of preventing the further spread of the outbreak, individuals still feared they would be negatively judged or scrutinized for the information needed to be disclosed.[54] Individuals were also reluctant to disclose the necessary information because of their concern for maintaining confidentiality and privacy.[55] Another limitation of the process is that it relies on what an individual remembers about her

[45] *Id.* at 16-17 (explaining that, with prostitution being thought of as the "reservoir of venereal diseases like syphilis," regulations, known as reglementation, were developed to authorize medical inspections of sex workers).
[46] *Id.* at 17.
[47] *Id.* at 16.
[48] *Id.* at 16-17.
[49] *Id.* at 24.
[50] Lehmann, *supra* note 40.
[51] *See* PRIV. INT'L, *supra* note 36.
[52] *See* Lehmann, *supra* note 40; *see generally* Kass & Gielen, *supra* note 36.
[53] Gostin et al., *supra* note 27, at 23.
[54] Lehmann, *supra* note 40.
[55] Gostin et al., *supra* note 27, at 26; *see generally* Lehmann, *supra* note 40.

whereabouts during the period of contagion.[56] These limitations cause traditional contact tracing to move even slower than it already typically does and ultimately prolongs the spread of the disease.

The contact tracing process inevitably relies on individuals' willingness to entrust public health departments to maintain confidentiality and protect one's privacy.[57] If the public does not trust that their information will remain private they can simply preserve their right to privacy by refusing to disclose the necessary information.[58] Privacy concerns are exacerbated because the "contacts" are under no obligation to maintain confidentiality.[59] Although healthcare workers do not disclose the index patient's name, the contacts may otherwise know who the infected person is and ultimately disclose that sensitive information to others.[60] The greater number of people who have the confidential information, the greater likelihood that an individual's privacy is at risk.[61] No matter what disease is at issue, the contact tracing process can only be effective if there are safeguards in place to maintain privacy and security of one's personal health information in order to assure there is public trust.[62] Effective contact tracing begins and ends with the trust of the people.

III. COVID-19 AND CONTACT TRACING

The world was confronted unexpectedly with another new and deadly infectious disease just in time to celebrate the start of a new year. SARS-CoV-2, also known as COVID-19, is a new coronavirus that was first identified in Wuhan, China in December 2019.[63] The United States first began seeing COVID-19 cases during late January and into February, all related to travelers from China who were oblivious of their

---

[56] Lehmann, *supra* note 40.
[57] Kass & Gielen, *supra* note 36, at 96.
[58] *Id.*
[59] *Id.*; Nancy E. Kass, *An Ethics Framework for Public Health*, 91 AM. J. PUB. HEALTH 1776, 1782 (Nov. 2001), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1446875/pdf/0911776.pdf.
[60] Kass, *supra* note 59, at 1779.
[61] *See* Kass & Gielen, *supra* note 36, at 96.
[62] Lehmann, *supra* note 40; *see* Laura Bradford et al., *Covid-19 Contact Tracing Apps: A Stress Test for Privacy, the GDPR, and Data Protection Regimes*, 7 J. L. & BIOSCIENCES 1, 8-11 (2020).
[63] *COVID-19 Overview and Infection Prevention and Control Priorities in non-US Healthcare Settings*, CTR. DISEASE CONTROL (Feb. 26, 2021), https://www.cdc.gov/coronavirus/2019-ncov/hcp/non-us-settings/overview/index.html#background.

unprecedented travel companion, COVID-19.[64] The first nontravel related case was confirmed on February 26th.[65] The world began seeing the number of cases grow exponentially and spread over significant geographical areas affecting a large percent of the population, which meant this epidemic had become a global pandemic.[66]

The Centers for Disease Control and Prevention ("CDC") has indicated that the virus is spread from person to person through "respiratory droplets produced when an infected person coughs, sneezes, or talks."[67] The virus has spread rapidly through unknowing asymptomatic carriers.[68] The incubation period for the virus is thought to be between two and fourteen days, with the most contagious period being a day or two before one starts having symptoms.[69] COVID-19, a respiratory disease, has caused a range of mild to severe symptoms.[70] Common symptoms that have been considered key indicators of having COVID-19 include difficulty breathing, loss of taste and smell, a dry cough and a fever over 100.4 degrees.[71] Some of those infected have showed no symptoms.[72] Other cases, unfortunately, have resulted in

---

[64] Michelle A. Jordan et al., *Evidence for Limited Early Spread of COVID-19 Within the United States, January-February 2020*, CTR. DISEASE CONTROL (June 5, 2020), https://www.cdc.gov/mmwr/volumes/69/wr/mm6922e1.htm?s_cid=mm6922e1_w.

[65] *Id.*

[66] *Pandemic vs Epidemic: What's the Difference?*, ROCHESTER REG. HEALTH: HEALTH HIVE (Mar. 27, 2020), https://hive.rochesterregional.org/2020/03/Pandemic-vs-Epidemic.

[67] *How to Protect Yourself & Others*, CTR. DISEASE CONTROL, https://www.cdc.gov/coronavirus/2019-ncov/prevent-getting-sick/prevention.html (last updated Aug. 13, 2021).

[68] Vogt, *supra* note 37.

[69] *Coronavirus Incubation Period*, WEBMD, https://www.webmd.com/lung/coronavirus-incubation-period#1 (last visited Feb. 19, 2021). The incubation period is the number of days between when one is infected with something and when one might see symptoms, which is used by health care professionals to decide how long people need to stay away from others during the outbreak. *Id.* This period will differ with every condition. *Id.*

[70] CTR. DISEASE CONTROL, *supra* note 63, at 2.

[71] *Symptoms of COVID-19*, CTR. DISEASE CONTROL https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html (last updated Feb. 22,2021).

[72] *Id.*

death.[73] Globally, there have been over two hundred and fifty million people infected with COVID-19 and over five million people have died from it.[74] More than forty-seven million cases have been reported in the United States, with over seven hundred and sixty thousand people dying from it.[75] These numbers reflect the state of the pandemic as of November 16, 2021.

The CDC has issued guidelines to help stop the spread of COVID-19, including a fourteen-day quarantine period if one has been infected or been exposed to someone who was infected.[76] Additionally, the CDC has recommended people to practice social distancing, wear a mask, and wash one's hands frequently.[77] Between March and April, many states took matters in their own hands by issuing "stay at home" orders in the hope to stunt the spread of the virus.[78] California, New Jersey, and New York were among the states that essentially went into a complete shutdown.[79] With only essential workers allowed to leave the house, the shutdowns caused the country to see an economic downturn, but also briefly slowed the spread of the virus.[80] Once states began loosening restrictions on travel and business operations, COVID-19 cases also began growing again, which was then amplified once flu season hit.[81] As of February 22, 2021, cases were still reaching record highs, with the United States having reported 500,000 deaths.

---

[73] *COVID-19 Death Data and Resources*, CTR. DISEASE CONTROL (Sept. 1, 2020), https://www.cdc.gov/nchs/nvss/covid-19.htm; *see* Vogt, *supra* note 37, at 1.
[74] *Number of COVID-19 Cases by Country*, JOHNS HOPKINS UNIV. MED. https://coronavirus.jhu.edu/map.html (last visited Nov. 16, 2021, 10:42 AM).
[75] *Covid in the U.S.: Latest Map and Case Count*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/coronavirus-us-cases.html (last visited Nov. 16, 2021, at 10:45 AM).
[76] *Quarantine and Isolation*, CTR. DISEASE CONTROL (last updated Oct. 19, 2021), https://www.cdc.gov/coronavirus/2019-ncov/your-health/quarantine-isolation.html.
[77] *Id.*
[78] Sarah Mervosh, Denise Lu, & Vanessa Swales, *See Which States and Cities Have Told Residents to Stay at Home*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html, (last updated Apr. 20, 2020).
[79] *Id.*
[80] *Id.*
[81] *Id.*

The CDC has further indicated, as it has for prior infectious disease outbreaks, that contact tracing would be an effective tool that would help identify potential asymptomatic carriers before they unknowingly spread the virus.[82] States that were seeing large influx of cases developed and implemented contact tracing plans early on, for example, New York's contact tracing program went in effect in May 2020.[83] The program was expected to have between 6,400 and 17,000 tracers statewide working remotely to gather information from an infected person.[84] The program had a baseline of thirty contact tracers for every 100,000 individuals.[85] In discussing New York's contact tracing program, Michael R. Bloomberg, Founder of Bloomberg Philanthropies and Bloomberg LP and former mayor of New York City, stated:

> One of the most important steps to take to re-open the economy as safely as possible is to create a system of contact tracing. When social distancing is relaxed, contact tracing is our best hope for isolating the virus when it appears and keeping it isolated. . . . [W]e are glad to support the state in developing and implementing a contact tracing program. And we will share what we learn publicly, so cities and states around the countries can build on our efforts, and so can nations around the world.[86]

[82] CTR. DISEASE CONTROL, *supra* note 32; *see also* Kelly Zegers, *NYC Public Advocate Seeks Contact Tracing Data Safeguards*, LAW360 (May 4, 2020), https://www.law360.com/articles/1269875/nyc-public-advocate-seeks-contact-tracing-data-safeguards.
[83] *Id.*
[84] *Id.*
[85] *Amid Ongoing COVID-19 Pandemic, Governor Cuomo Announces Contact Tracing Pilot Program Supported by Mayor Mike Bloomberg to Begin in Coming Weeks*, N.Y. STATE (Apr. 30, 2020), https://www.governor.ny.gov/news/amid-ongoing-covid-19-pandemic-governor-cuomo-announces-contact-tracing-pilot-program-support-0.
[86] *Id.*

The New York contact tracing program has been the leading partnering program in the nation.[87] The program has been implemented in coordination with New Jersey and Connecticut.[88]

Contact tracing for COVID-19 has required individuals to disclose more sensitive and private information than just recent sexual partners.[89] A person infected with COVID-19 must disclose anyone she has been in "close contact" with.[90] For COVID-19 contact tracing purposes, a close contact is someone "who was within 6 feet of an infected person for at least 15 minutes starting from 48 hours before illness onset until the time the patient is isolated."[91] The problem arises with how unsuspectingly COVID-19 spreads.[92] The virus can be transmitted before a person has symptoms, before she feels sick or even if she has very mild symptoms.[93] Because COVID-19 can be transmitted between people without the manifestation of symptoms, contact tracing has become complicated and time-consuming in its traditional form.[94]

Contact tracing has generally been the most effective when a disease is easily detected from its onset.[95] Because many are unaware of when they become infected, contact tracing professionals must work promptly and efficiently to notify as many potentially exposed people as possible in order to have a significant impact on stopping the spread of the COVID-19.[96] In Philadelphia, the contact tracing team reaches

---

[87] *State Approaches to Contact Tracing during the COVID-19 Pandemic*, NAT'L ACAD. STATE HEALTH POL'Y, https://www.nashp.org/state-approaches-to-contact-tracing-covid-19/ (last updated Jan. 21, 2021).
[88] N.Y. STATE, *supra* note 85.
[89] Vogt, *supra* note 37; *see also* Gostin et al., *supra* note 27 ("The Centers for Disease Control and Prevention (CDC) recommends that persons living with HIV disclose their HIV status to potential sexual and needle sharing partners, and supports public health strategies to facilitate disclosure.").
[90] Radcliffe, *supra* note 32.
[91] *Id.*
[92] *Id.*; *see* Jennifer Steinhaure et al., *Contact Tracing Is Failing in Many States. Here's Why.*, N.Y. TIMES, https://www.nytimes.com/2020/07/31/health/covid-contact-tracing-tests.html (last updated Oct. 5, 2020).
[93] Radcliffe, *supra* note 32.
[94] *Tracking COVID-19: Contact Tracing in the Digital Age*, WORLD HEALTH ORG. (Sept. 9, 2020), https://www.who.int/news-room/feature-stories/detail/tracking-covid-19-contact-tracing-in-the-digital-age.
[95] Steinhaure et al., *supra* note 92.
[96] *Id.*

80% of the named contacts they call and they complete 80% of the interviews for those contacts.[97] The contact tracing team in Maine has also reported a 96% success rate in getting contacts to agree to enroll and be automatically monitored to see if they develop COVID-19.[98]

The distinct nature of COVID-19, however, caused some contact tracing efforts overburdened by the inability to keep up with the rapid increase of cases.[99] The contact tracing process cannot begin without a positive test result and in some areas results are taking upwards of nine days to come back.[100] This delay diminishes the ability to do contact tracing because the infectious period has now ended and would render tracers' efforts practically moot.[101] The process is also ineffective if people are unwilling to participate.[102] In Maryland, about 25% of those contacted did not even answer the phone.[103] In Florida, tracers reported only reaching about 18% of those contacted who were infected in a given two week span, meaning 80% of infected people were not told by the tracers to isolate nor their close contacts informed of potential exposure.[104] Between the delay in test results, people's lack of cooperation, and the unique nature of COVID-19, traditional contact tracing has not been the wheelhouse solution it has been over the centuries in the face of this deadly coronavirus.

Although traditional contact tracing has not been as historically effective against COVID-19, it will not be completely replaced.[105] Experts, such as Dr. Anthony Fauci, Director of the National Institute of Allergy and Infectious Diseases, indicate that "widespread public health surveillance is essential to containing the deadly coronavirus."[106]

---

[97] Christine Lehmann, *COVID Surge Wrecks Contact Tracing Efforts*, WEBMD (Dec. 14, 2020), https://www.webmd.com/lung/news/20201214/covid-surge-wrecks-contact-tracing-efforts.

[98] *Id.*

[99] *See* Radcliffe, *supra* note 32; *see* Steinhaure et al., *supra* note 92.

[100] Steinhaure et al., *supra* note 92.

[101] *Id.*

[102] Lehmann, *supra* note 40.

[103] Steinhaure et al., *supra* note 92.

[104] *Id.* (The statics do not account for those who were deemed infected that could have been told by family, peers, etc. to isolate).

[105] Volkin, *supra* note 9; *see also* Radcliffe, *supra* note 32. ("[A]pp-based tracing won't replace manual contact tracing entirely.").

[106] Vogt, *supra* note 37; *see also* Zegers, *supra* note 82. ("[T]he tracking of whose had contact with COVID-19 positive individuals – is a critical step to getting out from under the pandemic, but said data needs to be collected in a

In fact, traditional contact tracing is being enhanced through the use of technology to assist in meeting the goal of widespread surveillance.[107]

IV. DIGITAL CONTACT TRACING

Digital contact tracing provides the widespread public health surveillance that Dr. Fauci and other experts insist is necessary to stop the spread of COVID-19.[108] Together, COVID-19 testing and the use of geolocation technology for contact tracing can be the answer for life to return to normal.[109] Digital contact tracing relies on individuals' mobile devices to collect data about an individual's whereabouts.[110] Contact tracing apps have been developed using either Bluetooth or GPS technology.[111] Each of these technologies provide a way of notifying an individual that she has been exposed to or in close contact with a person that has indicated she has COVID-19.[112]

The digital contact tracing process differs depending on whether an app is Bluetooth based or GPS based.[113] Apps using Bluetooth have markers that are designed to determine whom you came into contact with.[114] This form of digital contact tracing has been likened to a virtual "handshake."[115] In contrast, apps using GPS can track where a potentially infected user has been, at what time, and then match up with other users whose devices were at the same location during that time.[116]

---

way that doesn't do harm and doesn't allow information to end up in the 'wrong hands.'").

[107] *See generally* Volkin, *supra* note 9; Vogt, *supra* note 37.

[108] Boris Segalis & Jonathan Newmark, *Road Map for A Cautious Approach to Contact Tracing*, LAW360 (Apr. 30, 2020), https://www.law360.com/articles/1267979/road-map-for-a-cautious-approach-to-contact-tracing.

[109] *Id.*

[110] *Id.*; *see also* PRIV. INT'L, *supra* note 36.

[111] Cattanach et al., *supra* note 14.

[112] *Id.*

[113] *Id.*

[114] *Id.*; *see also* Sam Biddle, *The Inventors of Bluetooth Say There Could Be Problems Using Their Tech For Coronavirus Contact Tracing*, INTERCEPT (May 5, 2020, 6:00 AM), https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing/; *see generally* Christine Julien, *Contact-tracing apps for COVID-19: What You Need to Know (and Do)*, YAHOO (May 19, 2020), https://news.yahoo.com/contacttracing-apps-for-covid-19-what-you-need-to-know-and-do-090057070.html.

[115] Cattanach et al., *supra* note 14; *see also* Bradford et al., *supra* note 62.

[116] Cattanach et al., *supra* note 14; *see also* Bradford et al., *supra* note 62.

GPS location data can provide tracking information of potential outbreaks or hotspots.[117] With both technologies, if two or more people with the app installed spend a significant amount of time (CDC suggests longer than fifteen minutes[118]) within the minimum distance of each other (commonly six feet[119]), their smartphones create and store an anonymous record of that contact.[120] Then, if someone updates the app to indicate she has been infected, the app uses that stored information and sends a warning to any person she has had extended contact with.[121] As compared to traditional contact tracing, digital contact tracing is necessarily invasive, but it is not labor intensive. Contact tracing apps perform the work of collecting and retaining the personal information that is necessary to track and identify close contacts.[122] The information these apps need to be effective include geolocation, proximity to others, biometrics and health care diagnosis.[123] Because the apps have the capacity to store this information, the contact tracing process is not constricted to only what an individual can remember.[124] Therefore, more contacts can be identified and automatically notified of the potential exposure. [125]

Although the United States has not adopted a blanket digital contact tracing method, many countries have implemented digital contact tracing methods as part of their response to the pandemic.[126] For

---

[117] Cattanach et al., *supra* note 14.
[118] CTR. DISEASE CONTROL, *supra* note 32.
[119] *Id.*
[120] Thorin Klosowski, *COVID Contact Tracing Apps Are Far From Perfect*, WIRECUTTER (Nov. 2, 2020), https://www.nytimes.com/wirecutter/blog/covid-contact-tracing-apps/; *see also* Ron Raether et al., *Privacy Guidelines For COVID-19 Contact-Tracing App Markers*, LAW360 (Apr. 17, 2020, 5:43 PM), https://www.law360.com/articles/1264669/privacy-guidelines-for-covid-19-contact-tracing-app-makers.
[121] Klosowski, *supra* note 120.
[122] Raether et al., *supra* note 120.
[123] *Id.*
[124] PRIV. INT'L, *supra* note 36; *see also* Fanny Anderson, *Digital Contact Tracing – Advantages, Risks & Post-COVID Applications*, DECIBIO: INSIGHTS (Aug. 25, 2021), https://www.decibio.com/2020/04/14/digital-contact-tracing-2020-4-14/. ("Digital tracing provides a more scalable approach to traditional contact tracing, which relies on patients' memories of recent exposure to others.")
[125] PRIV. INT'L, *supra* note 36; Anderson, *supra* note 124.
[126] Raether et al., *supra* note 120.

example, China has made the use of Alipay Health Code mandatory for all citizens.[127] The Alipay Health Code app uses quick response codes to track infected citizens as they pass checkpoints around the city in order to regulate movement within quarantine zones.[128] Additionally, citizens are given a color code each day that informs them whether they are authorized to travel.[129] Similar to China, Israel requires all citizens to use the application Hamagen, which tracks a user's location and alerts that user if she has been in the vicinity of someone who has been diagnosed with COVID-19.[130] In contrast, Singapore has implemented digital contact tracing methods on a voluntary basis through the use of Bluetooth technology.[131] Many European countries have also begun using contact tracing apps, all on a voluntary basis.[132]

Voluntary use of contact tracing apps is the most democratic way of implementing these new COVID-19 fighting methods, but it is not without its' downsides. The most stringent and apparent problem is people are not voluntarily downloading the app.[133] For example, in Singapore only about "one in six people in the country had actually downloaded the app a few weeks after it was available."[134] In Iceland, an app was launched in April 2020 and by July 8, 2020 the "adoption rate was less than 40%."[135] On August 24, 2020, Nevada launched

---

[127] *Id.;* Anderson, *supra* note 124.
[128] *Id.*; Paul Mozur et al., *In Coronavirus Fight, China Gives Citizans a Color Code, With Red Flags*, N.Y. TIMES, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (July 26, 2021).
[129] Raether et al., *supra* note 120; Mozur *supra* note 128.
[130] Raether et al., *supra* note 120.
[131] *Id.*
[132] *Digital Solutions During the Pandemic*, EUR. COMM'N, https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/digital-solutions-during-pandemic_en (last visited Feb. 19, 2021).
[133] Lokke Moerel, *Contact Tracing Apps: Why Tech Solutionism and Privacy by Design are not Enough*, IAPP (May 7, 2020), https://iapp.org/news/a/contact-tracing-apps-why-tech-solutionism-and-privacy-by-design-are-not-enough/.
[134] Cristina Hernández-Quevedo et al., *How Do Countries Structure Contact Tracing Operations and What Is the Role of Apps?*, COVID- 19 HEALTH SYS. RESPONSE MONITOR (June 18, 2020), https://analysis.covid19healthsystem.org/index.php/2020/06/18/how-do-countries-structure-contact-tracing-operations-and-what-is-the-role-of-apps/.
[135] Chiara Farronato et al., *How to Get People to Actually Use Contact-Tracing Apps*, HARV. BUS. REV. (July 15, 2020),

COVID Trace, which was one of the nation's first COVID-19 contact tracing app.[136] State health authorities indicated that all several million Nevadans were strongly recommended to download the app.[137] However, as of November 9, 2020, only about 70,000 people had downloaded the app, which is about 3% of the state's adult population.[138]

The difficulty in having participation in contact tracing apps be voluntary is that such a high percentage of people must be willing to do so in order for this technology to be effective.[139] Researchers have estimated that 60% of the population needs to participate in order for contact tracing apps to be effective in stopping the spread of COVID-19.[140] This does not take in consideration those that do not own smartphones.[141] It is estimated that 81% of U.S. adults have smartphones.[142] With about 19% of adults not having smartphones, 74% of smartphone owners would need to participate in contact tracing apps in order to meet the effective adoption rate of 60%.[143] While mandating participation in contact tracing apps presents concerns under the Fourth Amendment, even voluntary use presents trepidation in the

---

https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps.

[136] 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/.

[137] *Id.*

[138] *Id.*

[139] NANCY AYER FAIRBANK ET AL., BERKMAN KLEIN CTR., THERE'S AN APP FOR THAT: DIGITAL CONTACT TRACING AND ITS ROLE IN MITIGATING A SECOND WAVE 19 (May 8, 2020), https://cyber.harvard.edu/sites/default/files/2020-05/Contact_Tracing_Report_Final.pdf.

[140] *Id.*; Mike Feibus, *Are Coronavirus Contact Tracing Apps Doomed to Fail in America?*, USA TODAY (June 24, 2020, 6:34 PM), https://www.usatoday.com/story/tech/columnist/2020/06/24/apple-google-contact-tracing-apps-privacy/3253088001/.

[141] FAIRBANK ET AL., *supra* note 139.

[142] *Id.*; Ashkan Soltani et al., *Contact-Tracing Apps are not a Solution to the COVID-19 Crisis*, BROOKINGS: TECHSTREAM (Apr. 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[143] FAIRBANK ET AL., *supra* note 139, at 3.

public that this type of surveillance will still have an impact on our civil liberties, such as our right to privacy.[144]

V. UNDERLYING CONCERNS WITH DIGITAL CONTACT TRACING

It should not come as a surprise that, like traditional contact tracing, digital contact tracing has raised some serious red flags at the onset of its conception. The type of mass surveillance that experts, such as Dr. Anthony Fauci, call for to stop the spread of COVID-19 is even more intrusive than having to disclose one's sexual partners.[145] Digital contact tracing apps will collect and retain information on where individuals have been, who they have been near, what symptoms they have, and monitor their health.[146] With a track record of "breaking public trust and violating citizen's privacy interest", the public has reason to question the consequences that this accumulation of data might cause, especially since data collection has never been done on such a mass scale before.[147] While he supports of mass surveillance from a public health standpoint, Dr. Anthony Fauci has considered concerns about civil liberties and has stated, "Do you give up a little liberty to get a little protection? . . . [I]t was Benjamin Franklin, I think. He says, '[i]f you give up some liberty for some protection, you are neither free nor protected.'"[148]

This mass surveillance has society fearful that it will lead to the deterioration of civil liberties, such as the right to privacy.[149] Contact tracing apps are also concerning because Big Tech companies will have the opportunity to access private health information and the uncertainty as what consequences there will be for misusing it.[150] Concurrently, this

---

[144] FAIRBANK ET AL., *supra* note 139, at 27.
[145] Vogt, *supra* note 37.
[146] Cattanach et al., *supra* note 14; *see also* Vogt, *supra* note 37. ("Location data contains an enormously invasive and personal set of information about each of us, with the potential to reveal such things as people's social, sexual, religious and political associations.").
[147] FAIRBANK ET AL., *supra* note 139 at 22; PRIV. INT'L, *supra* note 33.
[148] Rachel Kraus, *Dr. Fauci points to 'civil liberty' implications of Google and Apple contact tracing*, MASHABLE (April 15, 2020) https://mashable.com/article/dr-fauci-civil-liberties-apple-google-contact-tracing.
[149] *See* Segalis & Newmark, *supra* note 108.
[150] Zegers, *supra* note 82.

type of data collection also poses a substantial risk to vulnerable communities.[151]

Individuals are unwilling to download digital contact tracing apps because they do not trust their privacy will be protected.[152] In a study commissioned by Avira, a security software vendor, 71% of Americans indicated they would not use COVID-19 contact tracing apps, with many citing privacy issues as their reasoning.[153] A report from the American Civil Liberties Union stated, "[l]ocation data contains an enormously invasive and personal set of information about each of us, with the potential to reveal such things as people's social, sexual, religious and political associations. . . . The potential for invasions of privacy, abuse and stigmatization is enormous."[154]

Individuals are signaling this distrust by not downloading contact tracing apps and thus guaranteeing one's information is safe from the hands of Big Tech companies and the government.[155] The desire to protect one's privacy is outweighing the need to protect public health from the rapid spread of COVID-19. After all, "[p]aradoxically, privacy is a public value" that "begins with personal choices about what individuals share, and with whom. But the cumulative impact of those judgements far exceeds the sum of their parts."[156] Without public trust, digital contact tracing cannot be the effective weapon in the fight against COVID-19 that experts plead it can be.[157]

---

[151] *Id.*

[152] Christopher Longhurst, *Opinion: There's an Added Protection Against COVID-19 That Fits in Your Pocket. Why Aren't You Using It?*, SAN DIEGO UNION-TRIB. (Jan. 26, 2021, 5:10 PM), https://www.sandiegouniontribune.com/opinion/commentary/story/2021-01-26/ca-notify-app-covid-19.

[153] Kat Jercich, *Survey says majority of Americans won't use COVID-19 contact-tracing apps*, HEALTHCARE IT NEWS (June 16, 2020), https://www.healthcareitnews.com/news/survey-says-majority-americans-wont-use-covid-19-contact-tracing-apps.

[154] Vogt, *supra* note 37.

[155] Jercich, *supra* note 153.

[156] Laurence Tribe, *Digital coronavirus data tracing would barter away American liberties*, USA TODAY (Apr. 22, 2020, 12:12 PM), https://www.usatoday.com/story/opinion/todaysdebate/2020/04/21/coronavirus-data-tracing-barter-away-liberties-laurence-tribe-editorials-debates/3000576001.

[157] Yoshua Bengio et al., *The Need for Privacy with Public Digital Contact Tracing During the COVID-19 Pandemic*, 2 THE LANCET 7 (June 2, 2020),

The lack of trust the public has in Big Tech companies and the government in protecting their privacy stems from the prior mishandlings of data and information.[158] Historically, Big Tech companies have abused and misused the data they have collected for purposes other than those officially stated by them.[159] "Indiscriminate collection of personal information, chronic privacy breaches, and lax attitudes towards individual privacy in the private sector have eroded public trust in digital technologies."[160] Simply because the personal data being collected is necessary to help stop the pandemic, does not ensure it is free from the risk of "unauthorized disclosures, uses or misappropriation by unauthorized third parties, such as hackers."[161] For example, in December 2020, hackers "stole COVID-19 vaccine data belonging to Pfizer and BioNTech from the European Medicines Agency."[162] The hackers manipulated the exfiltrated data before it was leaked to undermine public trust in the vaccine.[163]

There is additional concern because contact tracing apps will give Big Tech companies access to private health information.[164] Personal health information is among the data that contact tracing apps will collect and retain, increasing the role large tech firms play in our health care sector.[165] In a letter to the White House, U.S. Senator Mark R. Warner, Senator Richard Blumenthal, and U.S. Rep. Anna Eshoo stated, "these partnerships [health and technology companies] have bolstered the platforms' ability to exploit consumer data and leverage their hold on data into nascent markets such as health analytics."[166] Without a comprehensive federal privacy law and numerous state privacy laws, there is no clear platform that would regulate the means

---

https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30133-3/fulltext.

[158] Vogt, *supra* note 37.

[159] *Id.*

[160] Bengio et al., *supra* note 157.

[161] Vildan Altuglu et al., *Assessing Heath Data Privacy Damages During a Pandemic*, LAW360 (Sept. 8, 2020, 4:53 PM), https://www.law360.com/articles/1306990.

[162] Jessica Davis, *COVID-19 Vaccine Data Manipulated Before Leak to Impair Public Trust*, HEALTH IT SEC. (Jan. 19, 2021), https://healthitsecurity.com/news/covid-19-vaccine-data-manipulated-before-leak-to-impair-public-trust.

[163] *Id.*

[164] Vogt, *supra* note 37.

[165] *See id.*

[166] *Id.*

contact tracing apps collect, store and retain data. Additionally, personal health information is afforded more legal protection that presently Big Tech companies are not obligated to abide by.[167] In a poll of patients and consumers from Morning Consult and America's Health Insurance Plans, 90% reported that they want technology companies held to the same high standard and scrutiny as health insurance providers when it comes to protecting their information.[168] Therefore, if the public does not trust Big Tech companies having access to less valuable information, so one would not expect the public to willing take the additional risk of disclosing health information.[169]

Additionally, contact tracing apps pose substantial risk for vulnerable communities, such as undocumented immigrants.[170] Undocumented immigrants seem to be hesitant to share location information without some assurance that this information will not be used for anything other than its intended purpose.[171] It is these vulnerable communities that are developing the most sever COVID-19 cases because of intricacies of poverty, limited access to healthcare, and fear of legal repercussions.[172] The concern for vulnerable communities is exacerbated because of the limited access to technology that the homeless and elderly population have.[173] Therefore, not only do contact tracing apps need to maintain privacy protections that provide safeguards for undocumented immigrants, there cannot be over reliance

---

[167] *Patients Believe Stronger Privacy Protections are More Importance Than Easier Health Data Access*, HELP NET SEC. (Jan. 27, 2020), https://www.helpnetsecurity.com/2020/01/27/health-data-access.
[168] *Id.*
[169] *Id.*
[170] Zegers, *supra* note 82.
[171] *Id.*
[172] Eva Clark et al., *Disproportionate impact of the COVID-19 pandemic on immigrant communities in the United States*, PLOS NEGLECTED TROPICAL DISEASES, July 13, 2020, at 1, 6, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7357736/pdf/pntd.0008484.pdf.
[173] Radcliffe, *supra* note 32; *see also* Craig Timber et al., *Most Americans are not Willing or Able to Use an App Tracking Coronavirus Infections. That's a Problem For Big Tech's Plan to Slow the Pandemic*, WASH. POST (Apr. 29, 2020), https://www.washingtonpost.com/technology/2020/04/29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-techs-plan-slow-pandemic.

on technology so that the homeless and elderly are left to parish.[174] While digital contact tracing can be impactful against the spread of COVID-19, implementation of this technology must consider all vulnerable communities to ensure adequate public benefit.

The pressure for rapid epidemiological control of the pandemic has not been enough overlook the harsh reality that the public does not trust how Big Tech companies, or the government, will handle and protect their personal data and information.[175] Participation in contact tracing apps can be higher if privacy risks and concerns are adequately addressed from the very beginning of the development stage.[176] In the pursuit for the public to willingly share their information, contact tracing technology must be deliberately and systematically built with privacy protections at its core.[177] This can be done if Big Tech companies incorporate the principles of "Privacy by Design" into digital contact tracing technology.

VI. "PRIVACY BY DESIGN"

Even in times of a global pandemic, the handing and protection of personal information should not be overlooked, especially when there is an ethical and lawful solution that will secure our right to privacy.[178] Without a comprehensive federal privacy law and numerous differing state privacy laws, Big Tech companies, like Apple and Google, are taking the initiative in protecting our right to privacy by developing contact tracing technology that the public can trust.[179] "Privacy by Design" is the solution that can provide the public with the necessary assurance that their privacy will be protected while their information and data is being used to stop the spread of COVID-19.[180]

---

[174] Zegers, *supra* note 82; *see* Radcliffe, *supra* note 32.
[175] Zegers, *supra* note 82.
[176] Glob. Priv. Assembly's Exec. Comm., *Achieving Privacy by Design in Contact Tracing Measures*, GLOB. PRIV. ASSEMBLY (May 21, 2020), https://globalprivacyassembly.org/contact-tracing-statement.
[177] *In conversation with Dr. Ann Cavoukian, Exec. Dir., Global Priv. & Sec., by Design Centre, former Can. Priv. Commr.*, GRC WORLD FORUMS (Oct. 14, 2021), https://www.grcworldforums.com/business/in-conversation-with-dr-ann-cavoukian-executive-director-global-privacy-and-security-by-design-centre-former-canadian-privacy-commissioner/3006.article; Kulsum & Khan, *supra* note 12.
[178] Glob. Priv. Assembly's Exec. Comm., *supra* note 168.
[179] Rich, *supra* note 7; APPLE & GOOGLE, *supra* note 16.
[180] Glob. Priv. Assembly's Exec. Comm., *supra* note 167.

"Privacy by Design", an almost twenty-year-old goal and mantra, is a "framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible."[181] It is essentially an acknowledgement of the relationship between legal privacy protection and actual privacy protection in a computerized society.[182] The core functionality of "Privacy by Design" is to build in privacy intentionally and with forethought into networked data systems and technologies.[183]

"Privacy by Design," first introduced by Dr. Ann Cavoukian, Canada's Information & Privacy Commissioner, is based on several principles that raise the privacy bar beyond the standards set forth in the Fair Information Practices ("FIPs"), making it the highest global standard for privacy protection.[184] The seven principles are: 1) Proactive not Reactive; Preventative not Remedial, 2) Privacy as the Default, 3) Privacy Embedded into Design, 4) Full Functionality – Positive-Sum, not Zero-Sum, 5) End-to-End Security – Lifecycle Protection, 6) Visibility and Transparency, and 7) Respect for User Privacy.[185] Each principle is discussed below.

[181] GRC WORLD FORUMS, *supra* note 177.
[182] *Id.*
[183] *Id.* at 153; *see* CAVOUKIAN, *supra* note 10, at 3.
[184] CAVOUKIAN, *supra* note 10, at 1; *see* Dag Wiese Schartum, Note, *Making Privacy by Design Operative*, 24 INT'L. J. L. INFO. TECH. 151, 153 (2016).
[185] CAVOUKIAN, *supra* note 10, at 2; *see also The Role of Privacy by Design in Protecting Consumer Privacy*, CTR. DEMOCRACY TECH. (Jan. 28, 2010), https://cdt.org/insights/the-role-of-privacy-by-design-in-protecting-consumer-privacy-1/.

A. Proactive not Reactive; Preventative not Remedial[186]

"Privacy by design" requires the anticipation and prevention of privacy invasive events.[187] Therefore, there needs to be proactive, rather than reactive, measures implemented.[188] There is a typical mentality to wait for privacy risks to emerge and have remedies for resolving those privacy infractions only after they have occurred.[189] In the adverse, "Privacy by Design" is aimed at preventing privacy infractions from occurring in the first place.[190] The key to meeting this principle is recognizing that there is value and benefit in implementing strong privacy practices from the beginning and throughout development of technology.[191]

B. Privacy as the Default[192]

The objective of this principle is that an individual should not have to do anything in order for her data be protected.[193] The technology should not require action on the part of the individual to protect their privacy.[194] The principle of "Privacy as the Default" is particularly influenced by the following FIPs: purpose specification, collection limitation, data minimization, and use, retention and

---

[186] This principle implies there should be the following: "1) a commitment, at the highest levels, to set and enforce high standards of privacy – generally higher than the standards set out by global laws and regulation; 2) a privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement; and 3) established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways." CAVOUKIAN, *supra* note 10, at 2.

[187] *Id.*

[188] *Id.*; *see also* CTR. DEMOCRACY TECH., *supra* note 185; *see generally* Elisa Jillson, *Privacy During Coronavirus*, FED. TRADE COMM'N (June 19, 2020 10:32 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/06/privacy-during-coronavirus.

[189] CAVOUKIAN, *supra* note 10, at 2.

[190] *Id.*

[191] *Id.*

[192] Bradford et al., *supra* note 62.

[193] CAVOUKIAN, *supra* note 10, at 2.

[194] *Id.*; *see also* Nicole Olsen, *Implementing Privacy by Design*, PRIV. POLICIES (Jan. 5, 2021), https://www.privacypolicies.com/blog/privacy-by-design.

disclosure limitation.[195] Combining these initiatives reinforces the importance of privacy being the default setting and ultimately is aimed at achieving the highest standard of privacy protection.[196]

C. Privacy Embedded into Design

Privacy is embedded into the design and architecture of informational systems when it is essential to the core function of that system.[197] When embedding privacy into technology, it should be done in a holistic, integrative and creative way.[198] Considering additional and broader contexts when designing these systems would qualify as holistic.[199] To be integrative, all stakeholders and their interests should be consulted.[200] Creativity is necessary because embedding privacy

---

[195] CAVOUKIAN, *supra* note 10, at 2; *see also* Edith Ramirez, Commr., Fed. Trade Comm., Remarks at the Privacy by Design Conference (June 13, 2012), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf. (The FIPs that correlate to this "Privacy by Design" principle are as follows: "1) Purpose Specification: the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances, 2) Collection Limitation: the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes, 3) Data Minimization: the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized, and 4) Use, Retention, and Disclosure Limitation: the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.").

[196] CAVOUKIAN, *supra* note 10, at 2.

[197] *Id.* at 3; *see also* Kulsum & Khan, *supra* note 11.

[198] CAVOUKIAN, *supra* note 10, at 3.

[199] *Id.*

[200] *Id.*

could mean current choices are unacceptable and new choices need to be invented.[201]

D. Full Functionality – Positive-Sum, not Zero-Sum

"Privacy by Design" is not a zero-sum approach and seeks to include all legitimate interests and objectives of the technology, but seeks to go beyond just making declarations and commitments to securing privacy.[202] Because "Privacy by Design" takes a positive-sum tactic, unnecessary trade-offs are not made.[203] It permits full functionality, therefore "privacy designs . . . should not be introduced at the expense of system functionality."[204] The technology should still provide practical results while providing beneficial privacy protections for all parties.[205]

---

[201] *Id.* The following provides strategies when implementing this principal: "[1)] A systemic, principled approach to embedding privacy should be adopted . . . [it] relied upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigor, at every step in the design and operation; [2)] Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics; [and 3)] The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error." *Id.*

[202] CAVOUKIAN, *supra* note 10, at 3.

[203] *Id.*

[204] Schartum, *supra* note 184.

[205] *Id.* The following are the three key points under this "Privacy by Design" principle: "1) Full functionality should not be impaired when embedding privacy into a given technology, process, or system. All requirements should be optimized to the greatest extent possible; 2) Legitimate non-privacy objectives are embraced and should be accommodated in an "innovative positive-sum manner." There should not be competition between privacy and technical capabilities, design objectives, or genuine interests; and 3) Documentation of all interests and objectives must be clear. The functions that are desired should be articulated. The agreed upon and applied metrics and the trade-offs that are rejected for being unnecessary should be documented. The documentation should conclude with a solution that enables multi-functionality." *Id.*

E. End-to-End Security – Full Lifecycle Protection

Not only should privacy be considered at the beginning stages of technology development, but it should also be a theme throughout the entire lifecycle.[206] Strong security measures are essential for privacy and full lifecycle protection ensures that all data are securely retained and then securely destroyed once the data has fulfilled its intended purpose.[207] The "Security" principle requires entities to assume responsibility for the security of personal information.[208] These applied security standards must assure the confidentiality, integrity, and availability of personal data, including methods of secure destruction, appropriate encryption, and strong access control and logging methods.[209]

F. Visibility and Transparency – Keep it Open

It is through "Privacy by Design" that provides assurance that technology is operating according to the stated promises and objectives, which is subject to independent verification.[210] The components and operations of the technology should remain visible and transparent to all.[211] This principle can be achieved through accountability, openness, and compliance.[212] Visibility and transparency are essential for establishing accountability and trust.[213]

---

[206] CAVOUKIAN, *supra* note 10, at 4.
[207] *Id.*
[208] CAVOUKIAN, *supra* note 10, at 4; *see* Kulsum & Khan, *supra* note 11.
[209] *See generally* CAVOUKIAN, *supra* note 10, at 4.
[210] *See generally* CAVOUKIAN, *supra* note 10, at 4.
[211] CAVOUKIAN, *supra* note 10, at 4; *see* Kulsum & Khan, *supra* note 11.
[212] CAVOUKIAN, *supra* note 10, at 4.
[213] Raether et al., *supra* note 120. There is special emphasis on the following FIPs: "1) Accountability: the collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured, 2) Openness: openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals, and 3) Compliance: complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should

G. Respect for User Privacy – Keep it User-Centric

"Privacy by Design" requires keeping the interests of the individual uppermost.[214] This goal is achieved through such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.[215] Data subjects are encouraged to play an active role in the management of their own data as this can be an effective check against abuses and misuses of privacy and personal data.[216]

The "Privacy by Design" principles have been influential, in some capacity or another, in recommendations for privacy protection from the Federal Trade Commission ("FTC"), the construction of the California Consumer Privacy Act ("CCPA") and the Health Insurance Portability and Accountability Act ("HIPPA"), and even other international privacy laws.[217] Because of the myriad federal, state, and local privacy laws, Big Tech companies can use "Privacy by Design" to ensure contact tracing apps provide the highest standard for privacy protection, guarantee broad compliance and avoiding legal challenges.[218] The "Privacy by Design" principles should be incorporated into the development of contact tracing apps to provide the public assurance that the data and information collected will be protected.[219] If the public trusts that their privacy will be protected, then contact tracing apps can be an effective battle weapon in the fight to stop the spread of COVID-19. This trust begins with infusing the principles of "Privacy by Design" into the digital contact tracing technology.

---

be taken." CAVOUKIAN, *supra* note 10, at 5; *see also* Raether et al., *supra* note 120.

[214] CAVOUKIAN, *supra* note 10, at 5; *see also* Olsen, *supra* note 194.

[215] CAVOUKIAN, *supra* note 10, at 5; FED. TRADE COMM'N, *supra* note 188.

[216] CAVOUKIAN, *supra* note 10, at 5.

[217] Raether et al., *supra* note 120; *see also* FED. TRADE COMM., *supra* note 188. The FTC recently suggested privacy tips parallel to the "Privacy by Design" principles for collecting consumer data to help during the pandemic. *See* Segalis & Newmark, *supra* note 108. The CCPA supports the user-centric focus in "Privacy by Design." *ICYMI: Summary of CCPA*, IWORKGLOBAL, (Oct. 8, 2018), https://www.iworkglobal.com/data-privacy-by-design-3. The emphasis on security in HIPPA echoes the "Privacy by Design" principle on security. Greg Garner, *Understanding the 5 Main HIPPA Rules*, HIPPA EXAMS (Jan. 21, 2021), https://www.hipaaexams.com/blog/understanding-5-main-hipaa-rules/.

[218] Raether et al., *supra* note 120; *see also* CAVOUKIAN, *supra* note 10, at 1.

[219] Segalis & Newmark, *supra* note 108.

The Exposure Notification system ("ENS"), developed by Apple and Google, is an example of contact tracing technology that has successfully incorporated the principles of "Privacy by Design."[220] Since it is being considered the most superior option in securing privacy and security, the next section will take a closer look at the Exposure Notification system and how it functions.[221]

VII. EXPOSURE NOTIFICATION

In an effort to assist in stopping the spread of COVID-19, Apple and Google joined forces to develop a technology that would provide a quicker method of identifying infected individuals and those potentially exposed.[222] In a news release, Apple stated, "we wanted to help state public health authorities make apps that can notify people of possible COVID-19 exposure in a way that's more reliable, efficient and private."[223] On April 10, 2020, the pair announced their contact tracing technology, Exposure Notification.[224] Exposure Notification is an application programming interface ("API") that will require public health officials to develop an app in order to use it.[225] Exposure Notification differs from traditional contact tracing in that it does not permit direct tracing by public health officials, but instead allows people to be notified that they were exposed to someone who recently tested positive for COVID-19.[226] Apple and Google intentionally developed the Exposure Notification system so that it could be effective against COVID-19 and the public can trust that their personal data will be protected.[227] The privacy protections within the Exposure Notification are in direct accordance with the principles of "Privacy by Design," making it no surprise that this contact tracing technology is considered the superior option in securing privacy and security.[228]

Parallel to the first principle of "Privacy by Design," Apple and Google have taken a proactive, instead of reactive, approach by prioritizing data privacy and security in the earliest stages of Exposure

---

[220] APPLE & GOOGLE, *supra* note 16.
[221] Cattanach et al., *supra* note 14, at 23.
[222] Cattanach et al., *supra* note 14, at 22; Lehmann, *supra* note 40.
[223] Lehmann, *supra* note 40.
[224] APPLE & GOOGLE, *supra* note 16.
[225] Gidari, *supra* note 15.
[226] *Id.*
[227] *Id.*
[228] Cattanach et al., *supra* note 14, at 22–23.

Notification development.[229] The other principles of "Privacy by Design" are clearly apparent in the development, functionality and implementation of Exposure Notification.[230]

Exposure Notification, once enabled, will allow devices to "regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier".[231] The Bluetooth identifier is not tied to a person's identity, but rather is a random string of numbers that changes every 10 to 20 minutes.[232] Other devices will be listening for these beacons as well as broadcasting their own and once a device receives a beacon, it is recorded and stored solely on that device.[233] The system will periodically download a list of beacons that have been verified as belonging to people that have tested positive for COVID-19.[234] Each device will then check the list against its recorded and stored beacons to see if there are any matches.[235] If there is a match, the user is notified and advised of next steps.[236] The Exposure Notification system is a decentralized system that stores data about what "contacts" the device has made on each users' device, instead of a centralized system that would report all users' data to a central server.[237]

In accordance with "Privacy by Design" principle of "Full Functionality," Apple and Google were able to introduce privacy protections that did not jeopardize the functionality of the Exposure Notification system because the system is able to identify and inform users' of potential exposures in an encrypted way which maintains a high level of privacy.[238] Additionally, privacy is embedded into the

---

[229] Feibus, *supra* note 140.
[230] *See* Moerel, *supra* note 133; *see* Kirk, *supra* note 13.
[231] APPLE & GOOGLE, *supra* note 16.
[232] *Id.*; *see* Davey Winder, *How to Disable Apple and Google's COVID-19 Notifications on Your Phone*, FORBES (June 28, 2020, 8:59 AM), https://www.forbes.com/sites/daveywinder/2020/06/28/how-to-disable-apple-and-googles-covid-19-notifications-on-your-phone-coronavirus-tracking-and-contact-tracing-app/?sh=46b9cf317242.
[233] APPLE & GOOGLE, *supra* note 16; *see* Winder, *supra* note 232.
[234] Winder, *supra* note 232; *see* Cat Ferguson, *Do Digital Contact Tracing Apps Work? Here's What You Need to Know*, MIT TECH. REV. (Nov. 20, 2020), https://www.technologyreview.com/2020/11/20/1012325/do-digital-contact-tracing-apps-work-heres-what-you-need-to-know.
[235] Winder, *supra* note 232; Ferguson, *supra* note 234.
[236] Winder, *supra* note 232; Ferguson, *supra* note 234; *see* Gidari, *supra* note 15.
[237] Soltani, *supra* note 142.
[238] *See generally* CAVOUKIAN, *supra* note 10.

system because it uses random Bluetooth beacons that constantly change instead of using an individual's personal identifiable information.[239] Apple and Google considered all the stakeholders' concerns when developing the Exposure Notification system and addressed them in a creative way that still achieves the purpose of contact tracing.[240]

The Exposure Notification system includes safeguards that amount to purpose specification, collection limitation, data minimization, and use, retention and disclosure limitation, the fundamentals of the principle "Privacy as the Default." The purpose specification piece is met because a public health authority must develop an app, then receive approval to gain access to the Exposure Notification system and once the outbreak is under control the system can be disabled on a regional basis.[241] This expressly indicates that stopping the spread of COVID-19 is the sole purpose for the personal data that will be collected, used, retained and disclosed.[242] The collection limitation piece is recognized when a user opts-in to turning on Exposure Notification because information is provided as to how data will be used, who will have access, and what information will be collected, allowing the user to be able to make well-informed decision on whether to participate or not.[243] Because Bluetooth identifiers are random and rotate often, an individual's identify is protected, she is unable to be tracked, and in that process none of her personal identifiable information has been shared or monetized, accomplishing the goal of data minimization.[244] Use, retention and disclosure is limited because the Exposure Notification system keeps the identity of the person who has tested positive private, operates using a decentralized system, users can delete the stored data on their devices, and the system can be disabled when it is no longer needed.[245]

The principle of "Respect for User Privacy" entails using strong privacy defaults, appropriate notice, and empowering user-friendly

---

[239] *See* Gidari, *supra* note 15.
[240] *See generally* APPLE & GOOGLE, *supra* note 16; CAVOUKIAN, *supra* note 10.
[241] APPLE & GOOGLE, *supra* note 16.
[242] CAVOUKIAN, *supra* note 10.
[243] Juli Clover, *Apple's Exposure Notification System: Everything You Need to Know*, MACRUMORS (Feb. 21, 2021), https://www.macrumors.com/guide/exposure-notification/.
[244] Gidari, *supra* note 15; APPLE & GOOGLE, *supra* note 16.
[245] APPLE & GOOGLE, *supra* note 16.

options.[246] Exposure Notification offers the ultimate user-centric path by giving users the explicit choice to opt-in to turning the system on.[247] The system furthers the empowerment of the user by allowing users to it turn the system off and delete the stored data whenever an individual choses to do so.[248] Users must consent to allowing the public health authority access to a list of beacons provided by users confirmed as positive for COVID-19.[249] The Exposure Notification system does not share location data from an individual's device with the public health authority, Apple, or Google.[250] If a public health authority decides to create an app for contact tracing efforts, it must meet specific criteria around privacy, security, and data to even gain authorization to use the Exposure Notification System, ensuring that users can trust that their privacy will be protected even when using a government sponsored app.[251]

Furthermore, the Exposure Notification system satisfies the principle of "End to End Security" because it includes security standards such as secure destruction, appropriate encryption, and strong access control and logging methods.[252] Data destruction is secure because each device stores the collected Bluetooth beacons, and a user can make the explicit choice to delete that data.[253] A person's identity is encrypted through the random string of numbers that regenerates several times a day.[254] The system uses a secured method of logging because only public health authorities will have access to an individual's list of beacons if that individual tests positive with COVID-19 and consents to sharing it.[255] Apple and Google will not have access at all to these lists.[256] The information remains deidentified even once it is in the

[246] CAVOUKIAN, *supra* note 10.
[247] APPLE & GOOGLE, *Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19*, https://www.google.com/covid19/exposurenotifications/ (last visited Feb. 19, 2021); Segalis & Newmark., *supra* note 108.
[248] APPLE & GOOGLE, *supra* note 16.
[249] *Id.*
[250] CAVOUKIAN, *supra* note 10.
[251] APPLE & GOOGLE, *supra* note 16.
[252] CAVOUKIAN, *supra* note 10, at 6.
[253] Raether et al., *supra* note 120; Segalis & Newmark, *supra* note 108.
[254] Raether et al., *supra* note 120.
[255] APPLE & GOOGLE, *supra* note 16; Raether et al., *supra* note 120.
[256] APPLE & GOOGLE, *supra* note 16.

hands of the public health authority.[257] The system will share date with the public heath authority if one of the following scenarios occurs: 1) "a user chooses to report a positive diagnosis of COVID-19" or 2) "if a user is notified that they have come into contact with an individual who is positive for COVID-19."[258]

Visibility and transparency are essential for establishing accountability and trust, making this principle crucial in the development of contact tracing technology.[259] Apple and Google are demonstrating accountability and responsibility for users' data by requiring equivalent privacy protections through contractual obligations, such as prohibiting public health authorities from requesting or collecting device location.[260] Since the release of Exposure Notification, improvements have been made to the system to incorporate more compliant and effective features, such as a simpler on/off toggle at the top of the Exposure Notification page on a device and a periodic reminder that the system is still on.[261] The Exposure Notification system has been developed and implemented deliberately and systematically with privacy protections that assure the public their data is in safe hands. This trust is necessary for mass corporation in the digital contact tracing effort to stop the spread of COVID-19.

VIII. CONTACT TRACING APPS IN PRACTICE

The COVID-19 pandemic is still rampant throughout the United States with cases still increasing and with unique variants of the virus appearing there is no clear end in sight.[262] Presently, nineteen states, Washington D.C., Guam, and Puerto Rico have apps that employ the

---

[257] *Id.*

[258] *Id.*

[259] CAVOUKIAN, *supra* note 10, at 6.

[260] Dave Burke, *An Update on Exposure Notifications*, GOOGLE (July 31, 2020), https://blog.google/inside-google/company-announcements/update-exposure-notifications; see also CAVOUKIAN, *supra* note 10, at 5. ("Accountability: the collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate and assigned to a specified individual.").

[261] Burke, *supra* note 260.

[262] Emily Crane, *COVID-19: New, inefectious strain of Delta variant deteched in the US*, N.Y. POST (Oct. 20, 2021), https://nypost.com/2021/10/20/covid-19-new-strain-of-delta-variant-detected-in-the-us/ (last visited Nov. 17, 2021, 10:16 AM).

Exposure Notification system.[263] Even with the intentional privacy safeguards that the Exposure Notification system has, apps are still experiencing low adoption rates.[264] As of late November 2020, only about eight million people in the United States adopted contact tracing apps whereas German and England have reached over twenty million installations.[265] Some would consider the digital contact tracing efforts to be a complete failure since the pandemic is still in control of our lives.[266] However, the privacy protections embedded into the Exposure Notification system have made it an attractive digital contact tracing technology to utilize among the states that are turning to contact tracing apps to help stop the spread of COVID-19.[267] Time has also showed that any adoption rate can have an impact on decreasing the amount of people infected.[268] Other current factors that have contributed to low adoption rates will be further discussed below.

The adoption of contact tracing apps might not have spread like rapid fire as COVID-19 did across the nation, but the impact these apps have had should be noted. Early on in the pandemic, it was noted that contact tracing apps would need a 60% adoption rate in order to be effective against the spread of the virus.[269] It turns out that contact tracing apps start having a protective effect at much lower adoption rates.[270] For example, if the adoption rate of contact tracing apps is 15%, then there can be a 15% decrease in infections, which results to an 11% decrease in deaths.[271] Furthermore, college students are so willing

---

[263] APPLE & GOOGLE, *supra* note 16; Vasudevan & Panthagani, *supra* note 21.
[264] *Id.*
[265] *Id.*
[266] *See* Rich, *supra* note 7.
[267] Mia Sato, *Contact Tracing Apps Now Cover Nearly Half of America. It's Not Too Late to Use One.*, MIT TECH. REV. (Dec. 14, 2020), https://www.technologyreview.com/2020/12/14/1014426/covid-california-contact-tracing-app-america-states/.
[268] *See* Leswing, *supra* note 22; Vasudevan & Panthagani, *supra* note 19.
[269] Vasudevan & Panthagani, *supra* note 19.
[270] *Id.*
[271] *Id.* In a recent study, researchers simulated a series of COVID-19 infections in the capital of La Gomera, San Sabastian de la Gomera, to get a better understanding of whether the Rader COVID app technology could work in a real-world environment to contain a COVID-19 outbreak. The research indicated that 30% of the population adopted the technology and it was able to detect about six close contacts per infected person, over two times higher than the national average detected using manual contact tracing.

to use the contact tracing app that their school either piloted or endorsed that adoption rates are incomparable to those seen from nations and states worldwide.[272] For example, UC San Diego was the first of the University of California campuses to use the Google Apple EN Express app and over 50% of the campus population had activated the app.[273] College students are more technologically savvy, which has allowed them to better understand how exposure notifications apps have been deliberately and systematically built to preserve privacy.[274] With students having less apprehension using the apps and test result reporting remaining voluntary, trust has bolstered and privacy backlash has been avoided, resulting in UC San Diego's infection rate staying at less than one half percent since September.[275] Additionally, Michigan State University, using the exposure notification app MI COVID Alert, saw over 46,000 downloads across its campus and the surrounding county.[276]

Low adoption rates can be contributed to the slow development of contact tracing technology, such as the Exposure Notification system, limited public outreach and distrust of the new software from both states and users.[277] Many states did not want to put the time and resources into developing the technology therefore most of Americans did not even have the ability to opt in.[278] The introduction of Exposure Notifications Express ("EN Express") allows states a quick and easy way to "deploy a basic, pre-formatted version of the Apple/Google-enabled contact tracing apps, saving costs and development time."[279] States that have recently launched apps with EN Express have seen adoption rates that suggest there is still hope that this technology can

---

Further, the app's success was dependent on effective national and local communications campaigns to encourage people to use the app. *See* Emily Henderson, *Study Sheds New Light on Digital Contact Tracing to Control the Spread of COVID-19*, NEWS MED. LIFE SCIENCES (Jan. 27, 2021), https://www.news-medical.net/news/20210127/Study-sheds-new-light-on-digital-contact-tracing-to-control-the-spread-of-COVID-19.aspx.

[272] Vasudevan & Panthagani., *supra* note 19.

[273] *Id.*; *see also* Longhurst, *supra* note 152.

[274] Vasudevan & Panthagani., *supra* note 19.

[275] *Id.*

[276] *See id.*

[277] Alejandro De La Garza, *People Are Finally Downloading COVID-19 Exposure Notification Apps. Will they Make a Difference?*, TIME (Dec. 14, 2020 3:52 PM), https://time.com/5921518/covid-exposure-notification-apps.

[278] *See id.*

[279] *Id.*

still help mitigate the spread of COVID-19.[280] For example, California launched an EN Express app in early December and it was estimated that 13% of adults had opted in within the first day.[281]

Low adoption ratings have also been tied to lack of funding to advertise the apps.[282] States that have spent more per resident on advertising funding have seen higher adoption rates.[283] For example, Virginia has spent $0.18 per resident and had a 10.6% adoption rate, whereas Delaware spent $0.11 per resident and only had a 7.3% adoption rate.[284] In addition to having "Privacy by Design" inspired privacy safeguards, the EN Express app has the added benefit of allowing states to send push notifications directly to residents, which has led to higher adoption rates.[285] For example, California having the ability to send residents push notifications when the Exposure Notification system was available resulted in an unprecedentedly high adoption rate.[286]

It is easy to come to the conclusion that digital contact tracing efforts failed when even the Exposure Notification system, that was built deliberately and systematically with privacy protections from end-to-end, was unable to reach substantial adoption rates.[287] However, when considering that only until recently more than half of Americans did not even have access to an app, that many states still do not offer EN express or another app that uses the Exposure Notification system, and nothing is being advertised when an app is available, the picture becomes more clear as to why adoption rates are so low.[288] While the public trust is crucial for digital contact tracing methods to be effective against the spread of COVID-19, there needs to be additional effort from the federal and local governments that pave the way for the Exposure

[280] *Id.*
[281] *Id.*; *see also* Leswing, *supra* note 22. ("California is the most populous of the 19 U.S. sates so far to roll out an exposure notification system and is the state where both Google and Apple are headquartered.").
[282] De La Garza, *supra* note 277.
[283] *Id.*
[284] *Id.*
[285] Leswing, *supra* note 22.
[286] *Id.*
[287] Rich, *supra* note 7.
[288] Sato, *supra* note 267; Leswing, *supra* note 22; De La Garza, *supra* note 277.

Notification system and the like to even have the opportunity to assist in the fight against COVID-19.[289]

IX. CONCLUSION

Overlooking the infringement on our right to privacy during the pandemic could negatively impact our ability to resist future diminishment of privacy protection which is why pro-privacy technology, such as the Exposure Notification system, today is crucial in ensuring pro-privacy technology tomorrow. Now that a vaccination is available for COVID-19, the world is asking how an individual's vaccination status will be verified so that the pandemic can actually get under control.[290] How will employers be able to verify that employees have been vaccinated? Schools? Concert halls? Airports? Other states and countries? These questions have already led to the development of vaccine apps.[291] A vaccine app will allow an individual to quickly verify her vaccination status, permitting her to go to work or go on a European vacation.[292] Just as the Exposure Notification system has showed that technology can be effective even with sufficiently meeting the privacy principles outlined by "Privacy by Design", technology companies developing these vaccine apps are being encouraged to deliberately and systematically incorporate privacy safeguards into the core of the technology so that the public can trust their privacy will be protected.[293]

The Exposure Notification system has showed the most promise out of all the available digital contact tracing apps because it has been developed and implemented with the highest standard of privacy protections as suggested by "Privacy by Design". Although this technology has been slow to pick up steam, digital contact tracing will be around well after the pandemic is over and can be implemented in future outbreaks. Without a comprehensive federal privacy law and patchy state privacy laws, we must rely on Big Tech companies to protect our privacy, especially with sensitive healthcare data. That is why it is this author's opinion that "Privacy by Design" is a crucial

---

[289] Nadia Dreid, *Sen. Markey Urges White House to Make Contact Tracing Plan*, LAW360 (Apr. 23, 2020), https://www-law360-com.proxy.libraries.rutgers.edu/articles/1266929/sen-markey-urges-white-house-to-make-contact-tracing-plan.

[290] Raether et al., *supra* note 24.

[291] *Id.*

[292] *Id.*

[293] *Id.*

strategy that should be implemented by those developing these "health" technologies and as a guide when developing future privacy laws.