Cleveland-Marshall
College of Law Library

Cleveland State University
EngagedScholarship@CSU

Law Faculty Articles and Essays

Faculty Scholarship

2021

Just Plain Dumb?: How Digital Contact Tracing Apps Could've Worked Better (And Why They Never Got the Chance)

Brian E. Ray

Follow this and additional works at: https://engagedscholarship.csuohio.edu/fac_articles

 Part of the Health Law and Policy Commons, Privacy Law Commons, Public Health Commons, and the Science and Technology Law Commons

How does access to this work benefit you? Let us know!

This Article is brought to you for free and open access by the Faculty Scholarship at EngagedScholarship@CSU. It has been accepted for inclusion in Law Faculty Articles and Essays by an authorized administrator of EngagedScholarship@CSU. For more information, please contact research.services@law.csuohio.edu.

Just Plain Dumb?: How Digital Contact Tracing Apps Could've Worked Better (And Why They Never Got the Chance)

Brian Ray[*]

I. INTRODUCTION

Imagine if a major health system developed a unique app for detecting new cases of COVID-19 up to a week before the current, widely used Polymerase Chain Reaction (PCR) tests. Users of the app would be required to wear a smartwatch capable of tracking their heart rate for at least eight hours each day. They would also fill out a baseline questionnaire with their age, BMI, gender, race, ethnicity, occupation and medical history, as well as a daily questionnaire reporting any

[*]Leon and Gloria Plevin Professor of Law, Cleveland-Marshall College of Law. I am grateful to the Charles M. Koch Foundation, and Cleveland State University's COVID-19 Rapid Response Faculty Research Fund for generously supporting the research for this Essay and related projects and the editors of the Seton Hall Law Review, especially Avi Muller and Lilli Wofsy for their excellent editing and infinite patience.

COVID-19-related symptoms they are experiencing and results of any COVID-19 tests.[1]

Now consider an algorithm that could use a broader range of information that many wearable devices like smartphones, smartwatches, and Fitbit devices regularly collect, including heart rate, step counts, sleep patterns, and others, to identify that someone likely has contracted COVID-19 up to nine days before they show any symptoms.[2] Surely most individuals would applaud these new tools. They leverage the technologies many people routinely use, and the information they already regularly share with private companies, to potentially save lives and mitigate the devastating economic effects of the pandemic. Indeed, press accounts of these promising new technologies lauded them as potentially powerful new tools to control the spread of COVID-19.[3]

While each of these tools clearly raises privacy concerns, those concerns could be managed with relatively routine protections, like requiring informed consent and applying the kinds of controls already used to protect sensitive health information. We might even design some additional protections to ensure that identifiable information is immediately destroyed after it is processed and that only de-identified and aggregated data is kept for later analysis.

In light of the tremendous potential—the possibility of saving thousands of lives—it would seem unreasonable to declare that the privacy risks these tools pose should stop us from piloting them. We should at least try to save lives, even if the preliminary studies acknowledged the need to test these tools with much larger numbers of people to ensure they work (and that it seems clear the tools will require widespread testing to work well).[4] Likewise, it would be foolish to

---

[1] Robert P. Hirten et al., *Physiological Data from a Wearable Device Identifies SARS-CoV-2 Infection and Symptoms and Predicts COVID-19 Diagnosis: Observational Study*, 23 J. MED. INTERNET RES. 2, 4 (2021) .

[2] *See* Tejaswini Mishra, et al., *Pre-Symptomatic Detection of COVID-19 from Smartwatch Data*, 4 NATURE BIOMEDICAL ENGINEERING 1208 (Nov. 18, 2020), https://www.nature.com/articles/s41551-020-00640-6.pdf.

[3] *See*, *e.g.*, Megan Cerullo, *Smartwatches Can Help Detect COVID-19 Days Before Symptoms Appear*, CBS NEWS (Jan. 15, 2021), https://www.cbsnews.com/news/covid-symptoms-smart-watch/; Chance Miller, *New Studies Show How Apple Watch Can Help Detect COVID-19 Prior to Symptoms and Testing*, 9TO5MAC (Jan. 16, 2021), https://9to5mac.com/2021/01/16/apple-watch-covid-studies-detection; Darrell Etherington, *Mount Sinai Study Finds Apple Watch Can Predict COVID-19 Diagnosis up to a Week Before Testing*, TECH CRUNCH (Feb. 9, 2021), https://techcrunch.com/2021/02/09/mount-sinai-study-finds-apple-watch-can-predict-covid-19-diagnosis-up-to-a-week-before-testing.

[4] *See* Hirten et al., *supra* note 1; Mishra et al., *supra* note 2.

declare that these apps should never collect specific types of sensitive information that health authorities could use to combat the pandemic.

Yet, that is precisely what happened with early proposals during the COVID-19 pandemic. The possibility that digital contact tracing apps could collect personal information that most people already routinely share was dismissed by many as too invasive and risky in spite of the fact that these apps offered even stronger privacy protections than the tools just described and at least equal and possibly greater potential benefits to society.[5] At the same time, Google and Apple exerted their nearly complete control over the global smartphone market to force governments across the world to enforce the hasty consensus that digital contact tracing apps should be prohibited from collecting location or information other than anonymized Bluetooth identifiers designed to estimate if a user was exposed to the virus.

Much commentary on digital contact tracing and other tools has shown a puzzling resistance to thinking through how these apps could allow public health officials to responsibly collect information to aid their efforts in combating the virus while still respecting pre-existing privacy norms in the public health context. Instead, a confounding consensus has emerged that even basic information like location data should be off the table because of the privacy risks its collection raises even though public health authorities routinely collect and responsibly use that same information to combat the spread of infectious disease through manual contact tracing and other processes.[6] This consensus ignores both the privacy tradeoffs society routinely makes in the public health context to protect ourselves from far lesser threats, as well as the

---

[5] *See, e.g.*, Jane Bambauer & Brian Ray, *COVID-19 Apps Are Terrible—They Didn't Have to Be*, LAWFARE DIGITAL SOCIAL CONTRACT (Dec. 21, 2020), https://www.lawfareblog.com/covid-19-apps-are-terrible-they-didnt-have-be.

[6] *See, e.g.*, Dali Kafaar et al., *Joint Statement on Contact Tracing: Date 19th April 2020* (Apr. 19, 2020), https://giuper.github.io/JointStatement.pdf ("Bluetooth-based solutions for automated contact tracing are strongly preferred [over GPS location] when available."); World Health Org., *Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing: Interim Guidance* 3 (May 28, 2020), https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 ("[D]ata collection should not require the identity or location data of a user, or a time stamp of a proximity event."); Euro. Data Protection Board, *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak* (Apr. 21, 2020) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf; ("[C]ontact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used."); Paige M.. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, A.B.A. (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy (describing how private companies collect consumer location data).

creative approaches that were emerging to responsibly use location and other information while still protecting privacy.[7]

The result is that the digital contact tracing apps in operation today protect privacy at the expense of efficacy and equity. They are underpowered by design, undersubscribed and ironically untrusted in spite (or perhaps because) of the extraordinary measures these tech giants have taken to protect privacy.[8] As of early 2021, fewer than half of the states in the United States ("U.S.") have even proposed using a contact tracing or exposure notification app.[9] Even in those, download rates are low and usage rates even lower.[10] These miserable statistics seem to prove correct early critics who argued that proposals to use digital contact tracing to help combat the pandemic were, as one prominent technologist put it, "just plain dumb."[11]

But these statistics are based solely on experience with the specific system that Google and Apple develop. By design and policy, that system prevents health authorities from using these apps to collect the same kinds of information they already use to understand and prevent the spread of communicable disease. These same limits effectively shut down alternative models that were emerging and that proposed to responsibly collect other information that could have made these apps more effective and accessible. That same information is critical to help understand whether these apps work as well as how this disease and the apps themselves affect the most vulnerable communities.

This Essay describes how the privacy debate that emerged over digital contact tracing and Google's and Apple's decisions to strictly limit apps permitted to use their platforms resulted in undercutting their potential usefulness as a tool to combat the pandemic while still failing to engender trust in these tools as intended. Part II describes the

---

[7] *See infra* Part II.B.

[8] *See* Lindsay Muscato, *Why People Don't Trust Contact Tracing Apps and What to Do About It*, MIT TECH. REV. (Nov. 12, 2020), https://www.technologyreview.com/2020/11/12/1012033/why-people-dont-trust-contact-tracing-apps-and-what-to-do-about-it; 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), https://time.com/5905772/covid-19-contact-tracing-apps.

[9] *See* Zac Hall, *Which U.S. States Are Using Apple's Exposure Notification API for COVID-19 Contact Tracing?*, 9TO5MAC (Jan. 16, 2021), https://9to5mac.com/2021/01/16/covid-19-exposure-notification-api-states.

[10] *See* Muscato, *supra* note 8; De La Garza, *supra* note 8.

[11] Bruce Schneier, *Me on COVID-19 Contact Tracing Apps*, SCHNEIER ON SECURITY BLOG (May 1, 2020), https://www.schneier.com/blog/archives/2020/05/me_on_covid-19; *see also* Ashkan Soltani et al., *Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis*, BROOKINGS TECH STREAM (Apr. 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster.

Google-Apple exposure notification system that quickly became the dominant model for digital contact tracing in the U.S. and Europe and the alternatives that were emerging early in the pandemic that Google's and Apple's entries into digital contact tracing effectively preempted.

Part III briefly recounts the factors that resulted in the privacy consensus that emerged early in the pandemic and that the Google-Apple system embodies. That consensus developed out of legitimate concerns that the federal government, in particular, would use the pandemic to expand domestic surveillance in ways similar to the post-9/11 era, as well as the growing resistance to the exploitation of consumer data by large technology companies. Two related phenomena reinforced it. First, pre-existing concerns over expansion of police surveillance were intensified by extensive use of social media and other sources to surveil the Black Lives Matter protests in Spring 2020. Second, the growing resistance to government response efforts, including mask orders and lockdowns, created tremendous political opposition to any expansion of state power.

Part IV argues that a contextual understanding of privacy in the public health context generally, and this pandemic, specifically, would allow for potentially more effective apps that permit health authorities responsibly to collect and use more information. It compares the Google-Apple Bluetooth-only system with the original Safe Paths proposal to combine that Bluetooth proximity tool with location information to illustrate this. Part IV then explores how other types of information have the potential to make these apps even more powerful tools and why some of that information is critical to evaluating whether these tools are working and how they are affecting different communities.

Part V identifies a minimum set of principles that a pandemic privacy law should include to enable responsible use of data to protect public health during future pandemics. Such a law would enable responsible use of both individual and aggregate information while still protecting against the core privacy and equity concerns raised by digital contact tracing.

II. DIGITAL CONTACT TRACING

A. *The Google-Apple System*

Most commentary to date has focused on apps using the very specific system that Google and Apple adapted from similar early models and established as the de facto international standard for apps permitted to use the interoperable Bluetooth function they created.[12] These tech giants labeled their system as performing "exposure notification" or proximity tracking to distinguish it from traditional contact tracing.[13] The system allows users only to identify that they have come into close proximity with someone who has tested positive rather than providing the detailed location and other information collected in traditional contact tracing. Applications using the system—and more recently the hardware function embedded in smartphones using Apple's or Google's respective operating systems—allow users to turn on a Bluetooth function that operates in the phone's background by sending and storing on each user's device rotating identifiers or keys to anonymously identify a device.[14] These keys are collected when two or more users running the app come into close contact for a defined period of time, typically fifteen minutes. The app incorporates an algorithm to estimate the distance between users based on the strength of the Bluetooth signal received from another device. The keys do not include location, time, or any other identifying information, only the fact that there likely was a close contact with another anonymized user.[15]

In addition to limiting the information these apps collect, Google and Apple also have imposed a stricter set of policies on them than they place on run-of-the-mine consumer applications.[16] To start, they

---

[12] *See, e.g.*, Casey Newton, *Why Countries Keep Bowing to Apple and Google's Contact Tracing App Requirements*, THE VERGE (May 8, 2020), https://www.theverge.com/interface/2020/5/8/21250744/apple-google-contact-tracing-england-germany-exposure-notification-india-privacy; Apple and Google, *Exposure Notification: Bluetooth Specification, Preliminary—Subject to Modification and Extension, Apr. 2020 v1.2* (Apr. 2020) [hereinafter *Bluetooth Specification*], https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf.

[13] *See* Matthew Panzarino, *Apple and Google Are Launching a Joint COVID-19 Tracing Tool for iOS and Android*, TECHCRUNCH (Apr. 10, 2020), https://techcrunch.com/2020/04/10/apple-and-google-are-launching-a-joint-covid-19-tracing-tool.

[14] *See id.*; *see also Bluetooth Specification*, *supra* note 12.

[15] Panzarino, *supra* note 13.

[16] *See* Khari Johnson, *Apple and Google Prohibit Location Tracking in New Contact Tracing Guidelines*, VENTURE BEAT (May 4, 2020), https://venturebeat.com/2020/05/04/apple-and-google-prohibit-location-tracking-in-new-contact-tracing-guidelines; APPLE, *Exposure Notification APIs Addendum*, 1–3 (May 4, 2020) [hereinafter, *Apple*

prohibit apps using this tool from allowing users to enable the app to collect any information other than the Bluetooth keys. Apps also are required to store those keys on a user's device unless and until the user tests positive and separately consents to provide the stored keys to a server maintained by a public health authority. A public health authority must either develop the app or sponsor it and the companies permit only one app per state in the U.S.[17]

If your goal is to minimize privacy risks at any cost, then this approach makes sense. The system stores only anonymized information that is extremely difficult to connect to any other information to identify a user. It also gives users complete control over whether to share even that information with anyone, including public health authorities. Finally, it limits access to that information to health authorities and requires that health authorities provide an official code for users to self-identify as receiving a positive COVID-19 diagnosis.[18]

The problem is that several of these protections compromise the system's effectiveness. Using Bluetooth has several distinct advantages for contact tracing over alternatives like location tracking using GPS and cell tower data. Bluetooth operates by devices signaling each other rather than a satellite or cell tower so it can function underground and inside buildings. Bluetooth also is better suited than sources like GPS or Wi-Fi signals for estimating whether a person was within the six-feet distance epidemiologists agree is necessary for potential exposure.[19]

But collecting only Bluetooth-based proximity information without related context, especially location and time, reduces the app to doing only one thing: alerting a user that she may have been exposed to an infected person.[20] This substantially limits what both users and health authorities can do with the app. It also makes the app itself less reliable.[21]

Exposure Notification], https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf.

17 *See* Johnson, *supra* note 16; *Apple Exposure Notification*, *supra* note 16.

18 Johnson, *supra* note 16.

19 *See* Ramesh Raskar et al., *Contact Tracing: Holistic Solution Beyond Bluetooth* [hereinafter *Holistic Solution*], https://github.com/PrivateKit/PrivacyDocuments/blob/master/ContactTracingBeyondBluetooth.pdf; *see also* COVID SafePaths, *COVID-19 Contact-Tracing Mobile Apps: Evaluation and Assessment for Decision Makers*, at 12 [hereinafter *COVID SafePaths*], https://github.com/PrivateKit/PrivacyDocuments/blob/master/apps-evaluation.pdf.

20 *See Holistic Solution*, *supra* note 19; *COVID SafePaths*, *supra* note 19.

21 *See Holistic Solution*, *supra* note 19; Camera Culture Group, MIT Media Lab, *Adding Location Context to Apple/Google Exposure Notification Bluetooth API: MIT SafePaths Encryption Proposals for GPS + Bluetooth*, Ver. 0.1, (Apr. 26, 2020) [hereinafter *Adding Location Context*].

Manual contact tracing involves identifying where someone who has tested positive recently visited and whom they may have exposed.[22] Without collecting contextual information, including the location and time of potential exposures as measured by the Bluetooth signal, the Google-Apple system cannot be used by manual contact tracers either to identify potential new cases or augment a person's memory. That system also cannot provide other useful information like identifying infected spaces for decontamination or assist in predicting likely future infection hotspots.[23] Instead, Apple and Google have created an entirely separate, relatively unreliable, system that, at best, offers the possibility that new cases could be identified even before the traditional process.

Even that limited promise requires a significant number of people to download and start running the app on a regular basis. Early research on Bluetooth-only models suggested that close to 60% of smartphone users would need to use an app to substantially reduce the spread of the virus, although lower rates could have some impact.[24]

Bluetooth-only systems also are highly imprecise and create significant risk of both

incorrectly identifying a potential exposure (false positive) or failing to trigger a notification even after an epidemiologically significant contact (false negative).[25] Even in controlled settings, the signal strength naturally fluctuates itself and differs by device.[26] Signal strength is highly sensitive to where a person places their device as well as the surrounding environment. Simply rotating one's body or placing a device in a bag can significantly reduce the signal's strength resulting in a false negative.[27] Reflective surfaces, like a subway or train car, can amplify the signal, and Bluetooth also passes through many walls. Either situation can create a false positive alert.[28]

---

[22] *See COVID SafePaths*, *supra* note 19, at 6.

[23] *Holistic Solution*, *supra* note 19.

[24] *See* Patrick Howell O'Neill, *No, Coronavirus Apps Don't Need 60% Adoption to be Effective*, MIT TECH REVIEW (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download.

[25] *See Holistic Solution*, *supra* note 19; Jeremy Hsu, *Contact Tracing Apps Struggle to Be Both Effective and Private*, IEEE SPECTRUM (Sept. 24, 2020), https://spectrum.ieee.org/biomedical/devices/contact-tracing-apps-struggle-to-be-both-effective-and-private.

[26] Amy Robinson & Jim Waldo, *Technical Difficulties of Contact Tracing*, LAWFARE (Dec. 17, 2020), https://www.lawfareblog.com/technical-difficulties-contact-tracing.

[27] *Id.*

[28] *Id.*

False positives can overburden health systems where testing capacity is limited and can cause economic hardship if they trigger an unnecessary quarantine. False negatives may seem innocuous but risk creating a false sense of security that could embolden people to take greater risks.[29] More broadly, people are far less likely to use or trust a tool that does not work.[30] Indeed, paradoxically, by prioritizing privacy over efficacy, Google and Apple may well have undermined the very trust they intended to develop.

Furthermore, these same limitations that make the apps less useful and unreliable also make it impossible to directly assess whether they work.[31] Without allowing even the user herself to learn where and when a likely exposure occurred, it is impossible to determine whether the notification was accurate.[32] These limits also prevent health authorities from using the information to understand the disease better. And by prohibiting health authorities from collecting any other user information, the system also precludes any analysis of how different demographic groups are affected by the disease and the apps themselves.

B. *The Path Not Taken*

Before Google and Apple announced these restrictions, there was tremendous excitement about a range of creative possibilities for incorporating the interoperable Bluetooth standard they were developing into more sophisticated applications. These applications proposed to collect other potentially useful data, including symptoms to allow individuals to calibrate their own risk better when deciding whether to self-isolate and researchers to understand this new disease

---

[29] *Id.*

[30] *See* Gabriel Kaptchuk et al., *How Good is Good Enough for COVID19 Apps? The Influence of Benefits, Benefits, Accuracy, and Privacy on Willingness to Adopt*, ARXIV (May 20, 2020), https://arxiv.org/pdf/2005.04343.pdf.

[31] *See* Nicole Wetsman, *Contact Tracing Apps Promised Big and Didn't Deliver*, THE VERGE (Dec. 11, 2020), https://www.theverge.com/22168473/coronavirus-contact-tracing-apps-exposure-notification-covid-google-apple (noting that "because of the apps' focus on privacy, it may be nearly impossible to quantify how well they're actually able to help prevent disease").

[32] *See, e.g.*, *id.* (noting that researchers cannot identify "how many of the people who receive notifications on the apps follow isolation guidelines or get tested for COVID-19"); Mark Briers et al., *Demonstrating the Impact of the NHS COVID-19 App*, ALAN TURING INSTITUTE (Feb. 21, 2021), https://www.turing.ac.uk/blog/demonstrating-impact-nhs-covid-19-app ("The decentralised design of the app means that it is not possible to directly measure the number of notifications that each individual index case generates.").

better.[33] Rather than spurring that kind of innovation and allowing public health authorities to drive the configuration of these apps, Apple and Google effectively prevented their tool from doing anything other than exposure notification.

Many of these alternative apps envisioned incorporating the proximity advantages of the interoperable Google-Apple Bluetooth system with other information, especially the time and location information critical for contact tracing, to create a more effective tool.[34] These apps also featured innovative approaches to protecting user privacy very differently from the one-size-fits-all model Apple and Google ultimately imposed.[35] Indeed, Google's public announcement seemed to anticipate such collaborations by noting that the second-phase plan to embed the Bluetooth tool into each company's operating system would "enable interaction with a broader ecosystem of apps and government health authorities."[36]

Safe Paths, a system developed by MIT researchers in consultation with the Mayo Clinic and spun off into the non-profit PathCheck Foundation, was one of the earliest and most prominent of these apps.[37] The original Safe Paths system included two components: (1) a smartphone-based app and (2) a centralized repository run by health authorities. The app was designed to collect both Bluetooth proximity information and GPS location data. As the Safe Paths team described in a series of publications, location information and Bluetooth-based proximity tools complement each other.[38] GPS systems provide location information which is useful for reconstructing where a person has

---

[33] *See*, *e.g.*, Hannah Alsdurf et al., *COVI White Paper-Ver. 1.1*, ARXIV (July 27, 2020), at 17–20, https://arxiv.org/pdf/2005.08502.pdf; Erman Ayday et al., *ShareTrace: A Smart Privacy-Preserving Contact Tracing Solution by Architectural Design During an Epidemic*, Ver. 1.0 (May 3, 2020), at 11, https://github.com/SafeTrace-community/info/blob/master/ShareTrace%20-%20WhitePaper_may3.pdf.

[34] *See, e.g.*, *Maximizing Privacy and Effectiveness in COVID-19 Apps*, OPENMINED (Mar. 24, 2020) [hereinafter *Maximizing Privacy*], https://blog.openmined.org/covid-app-privacy-advice (describing multiple app proposals and advocating for a multi-function, privacy-protective app).

[35] *See generally id.*; *see also* Ramesh Raskar et al., *Apps Gone Rogue: Maintaining Personal Privacy in an Epidemic,* ARXIV (Mar. 19, 2020) [hereinafter *Apps Gone Rogue*], https://arxiv.org/pdf/2003.08567.pdf.

[36] Google, *Apple and Google Partner on COVID-19 Contact Tracing Technology*, THE KEYWORD (Apr. 10, 2020), https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology.

[37] *Apps Gone Rogue*, *supra* note 35, at 66. Technical details and a series of whitepapers regarding Safe Paths and Safe Places are available on the PathCheck public GitHub site, https://github.com/Path-Check (PathCheck GitHub), and the TripleBlind Safe Places GitHub site, https://github.com/tripleblindai/safe-places.

[38] *See* Pathcheck Github, *supra* note 37; *COVID SafePaths*, *supra* note 19; *Holistic Solution*, *supra* note 19.

traveled, but GPS signals are not sufficiently precise to determine if a person was within the six-foot distance required for exposure. Bluetooth systems are configured to estimate that six-foot distance but, as discussed above, often result in false positives and false negatives. Location and time information provide critical context that mitigates these errors by allowing an individual to consider where they were, who was around them and what they were doing when they were exposed.[39]

The second component of the Safe Paths system, called "Safe Places," provided a mechanism designed to permit users to consent to securely upload both the Bluetooth identifiers and GPS location information to a public health database as part of the manual contact tracing process when they test positive for COVID-19.[40] Contact tracers could use the GPS location information directly to confirm, correct and amplify a person's memory during the interview process.[41] After removing potentially sensitive locations as part of the interview, the remaining location information would be de-identified and aggregated to create public heat maps that allow both users and non-users to self-identify potential exposures. Public health authorities could also use de-identified and aggregated location information to model and predict the location of future hotspots.[42]

Safe Paths incorporated many of the same protections as Apple and Google. All information is collected on a user's device and automatically deleted after 14 days. If a user tests positive she could elect to provide some or all of the stored information with health authorities. Unlike Google and Apple, Safe Paths also creates a backend interface for health authorities to securely upload and process the information users provide and delete specific locations they did not want to include in the system. Raw data is then deleted, while only de-identified, aggregated information is stored and eventually could be published as a public heatmap.[43]

---

[39] Camera Culture Group, MIT Media Lab, *Adding Location Context to Apple/Google Exposure Notification Bluetooth API: MIT SafePaths Encryption Proposals for GPS + Bluetooth*, Ver. 0.1, Apr. 26, 2020 [hereinafter *Adding Location Context*].

[40] *See* Anil Ananthaswamy, *What Do Public Health Authorities Need for COVID-19? Thinking beyond Exposure Notification, Contact Tracing and Heatmaps*, PATHCHECK FOUNDATION BLOG, (May 5, 2020), https://www.pathcheck.org/en/blog/what-do-public-health-authorities-need-for-covid-19-thinking-beyond-exposure-notification-contact-tracing-and-heatmaps. Technical details regarding Safe Places are available on the PathCheck GitHub site. *See* PathCheck GitHub, *supra* note 37.

[41] *See Adding Location Context*, *supra* note 39, at 33.

[42] *See* Ananthaswamy, *supra* note 40.

[43] *Id.*

Safe Paths was one of many alternative approaches that proposed allowing users to collect potentially useful information while still protecting their privacy. Other apps proposed creating more refined risk scores for determining whether to seek testing or self-quarantine by combining self-reported symptoms with location and Bluetooth identifiers.[44] Still others envisioned incorporating additional functions.[45] It is an open question how well any of these approaches might have worked but by prohibiting these apps from using their new tool, and tightly restricting contact tracing apps generally, Google and Apple never gave them a chance.

III. WHAT WENT WRONG?

Early in the pandemic, the aggressive use of intrusive digital surveillance by China, South Korea, Israel, and other nations created legitimate fear that governments across the globe might use public health as a cover to expand surveillance.[46] These fears that health surveillance tools would be used for law enforcement purposes, rather than restricted solely to fighting the pandemic, were intensified by police use of mobile phone and social media information to identify and arrest people participating in Black Lives Matters protests. Those fears were intensified when some law enforcement officials conflated those efforts with contact tracing generally.[47]

---

[44] *See*, *e.g.*, Alsdurf et al., *supra* note 33, at 4 (describing a Canadian app called COVI's use of proximity and symptom tracking); Ayday et al., *supra* note 33, at 8 (proposing the use of proximity, location and symptom tracking).

[45] *See Maximizing Privacy*, *supra* note 34 (describing examples including "a white label COVID Alert App, private set intersection, a differential privacy wrapper, and private identity").

[46] Peter Swire, *Security, Privacy and the Coronavirus: Lessons From 9/11,* LAWFARE (March 24, 2020, 2:46 PM), www.lawfareblog.com/security-privacy-and-coronavirus-lessons-911; Natasha Singer & Choe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, N.Y. TIMES (Apr. 17, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

[47] Amos Toh & Deborah Brown, *How Digital Contact Tracing for COVID-19 Could Worsen Inequality*, JUST SECURITY (June 4, 2020, 2:25 PM), https://www.hrw.org/news/2020/06/04/how-digital-contact-tracing-covid-19-could-worsen-inequality; Andy Meek, *Minnesota Is Now Using Contact Tracing to Track Protestors, As Demonstrations Escalate*, BGR (May 30, 2020, 10:46 PM), https://bgr.com/2020/05/30/minnesota-protest-contact-tracing-used-to-track-demonstrators; Isobel Asher Hamilton, *Compulsory Selfies and Contact Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It's Part of a Massive Increase in Global Surveillance*, BUSINESS INSIDER (Apr. 14, 2020, 11:30 AM), https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3.

In fact, in the U.S., state and federal authorities did the opposite.[48] They actively distanced themselves from the use of digital contact tracing apps.[49] The privacy concerns about digital contact tracing dovetailed with the general politicization of other government pandemic control measures to make even apps using the extremely limited Google-Apple system controversial. Protests against shutdown orders and mask mandates extended to both manual and digital contact tracing. One widely shared Facebook post claimed that federal legislation to expand and fund manual contact tracing would "give the government the power to forcibly remove" children from their homes.[50] An Ohio lawmaker warned constituents that "[a]rmies of agents" will be "trained on Apple and Google technology to trace or track people" and will "forcibly isolate" anyone who tests positive and all of their contacts.[51] Only three states, including South Carolina, initially announced that they would develop an app using the Google-Apple system.[52] Shortly after South Carolina announced its plans to develop an app, lawmakers in the state responded by amending a COVID-19 spending bill to ban state agencies from using it.[53]

As lawmakers in the U.S. went out of their way to prevent adoption of digital health surveillance tools, press accounts routinely reinforced fears that the apps under development risked unchecked expansion of government surveillance.[54] Even stories about the Google-Apple system

---

[48] *See* Bambauer & Ray, *supra* note 5.

[49] *See id.*

[50] *See* Angelo Fichera, *False Claim of Forced Removals Under Contact Tracing Bill*, FACTCHECK.ORG (May 13, 2020), https://www.factcheck.org/2020/05/false-claim-of-forced-removals-under-contact-tracing-bill.

[51] Rep. Nino Vitale, FACEBOOK (May 12, 2020), https://www.facebook.com/Rep Vitale/posts/2898165580261473.

[52] *See* Kif Leswing, *Three States Will Use Apple-Google Contact Tracing Technology for Virus Tracking Apps*, CNBC, (last updated May 20, 2020 5:37 PM), https://www.cnbc.com/2020/05/20/three-states-commit-to-apple-google-technology-for-virus-tracking-apps.html.

[53] Dave Perera, *South Carolina Legislature Puts Coronavirus Apps on Hold*, MLEX (June 26, 2020, 5:00 PM), https://mlexmarketinsight.com/news-hub/editors-picks/area-of-expertise/data-privacy-and-security/south-carolina-legislature-puts-coronavirus-apps-on-hold.

[54] *See* Natasha Singer & Choe Sang-Hun, *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, N.Y. TIMES (Apr. 17, 2020), https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html; Mike Giglio, *Would You Sacrifice Your Privacy to Get Out of Quarantine?*, THE ATLANTIC (Apr. 22, 2020), www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172.

routinely ignored how it actually works in favor of repeating unfounded concerns that it poses grave privacy risks.[55]

Google's and Apple's early announcements of their plans to develop an interoperable Bluetooth standard had a direct chilling effect on the ecosystem of digital tools that were emerging. Simply by announcing their common standard in early April 2020, even before it was ready, they largely preempted plans that other groups, including Safe Paths, were making with governments in several jurisdictions to move forward with alternatives.[56]

Many groups continued to develop alternative models even after this announcement focused on the possibility of incorporating the interoperable Bluetooth standard these companies were creating.[57] Apple and Google's later announcement of the restrictions they were imposing, in particular prohibiting apps using their Bluetooth tool from collecting location or other information and permitting only one app in each jurisdiction, essentially shut down those efforts.[58]

---

[55] *See, e.g.*, Evan Halper, *Lawmakers Warn Coronavirus Contact-Tracing Is Ripe for Abusive Surveillance*, L.A. TIMES (Apr. 26, 2020), www.latimes.com/politics/story/2020-04-26/privacy-americans-trade-off-trace-coronavirus-contacts.

[56] Google and Apple announced their partnership on April 10, 2020, and promised to release the API that apps needed to use it in May. *See Google Partner on COVID-19 Contact Tracing Technology*, APPLE: NEWSROOM (Apr. 10, 2020) [hereinafter *See Google Partner*], https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology. I spoke with Steve Penrod, CEO of TripleBlind, one of the partners in the original Safe Paths group on Jan. 28, 2021. *See* TripleBlind Github, https://github.com/tripleblindai/privatekit. Penrod said that announcement immediately slowed down or completely stopped the initial rollouts of the app and plans they were developing in several communities. *See Conversation with Steve Penrod*, Author's Notes (on file with author). As late as March 18, 2020, Safe Paths was in discussions with the White House to obtain official support for their system. *See* Austin Barnes, *White House Expected to Endorse Kansas City-Built COVID-19 Exposure Tracking App*, STARTLAND NEWS (Mar. 18, 2020), https://www.startlandnews.com/2020/03/private-kit-safe-paths-triple-blind-covid-19.

[57] *See, e.g.*, Safe Paths Alliance, *Adding Location Context to Apple/Google Exposure Notification Bluetooth API: MIT SafePaths Encryption Proposals for GPS + Bluetooth*, PATHCHECK (May 5, 2020), https://www.pathcheck.org/en/blog/adding-location-context-to-apple-google-exposure-notification-bluetooth-api-mit-safepaths-encryption-proposals-for-gps-bluetooth. When this announcement came out, I was working with a group of researchers from Case Western Reserve University and the University College London on a proposal to integrate the Google-Apple Bluetooth tool into an app designed to collect location, self-reported symptoms and other information using a completely different set of privacy controls to create a sophisticated risk score. Our proposal anticipated incorporating the Apple-Google Bluetooth system to provide proximity information interoperable with other apps. *See* Ayday et al., *supra* note 33, at 11.

[58] *See, e.g.*, Erin Simpson & Adam Conner, *Digital Contact Tracing to Contain the Coronavirus*, CTR. FOR AM. PROGRESS: TECH. POL'Y (Apr. 22, 2020), https://www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-

These strict limits were both driven by and reinforced the puzzling consensus among many privacy experts that location information would not be useful for digital contact tracing. Ignoring recommendations by leading public health organizations, several institutions including the World Health Organization and the European Data Protection Board issued guidelines asserting that contact tracing apps do not require and should not collect location information.[59]

Beyond the direct effect on alternative apps hoping to use their system, Google's and Apple's announcements focused attention on a single tech-company-created paradigm for using digital contact tracing. This had three negative consequences. First, public concerns about these companies' past privacy practices and domineering use of their control of the mobile technology market raised suspicion that this was yet another attempt to exploit consumer data for profit.[60] Many press accounts simply ignored the privacy protections the system incorporated in favor of highlighting mistrust in big tech and incorrectly implying that the system would give these companies increased access to valuable health information when in fact their strict policy *prohibited* apps from sharing any information with them.[61] Indeed, when both

tracing-contain-coronavirus (stating that Google's and Apple's announcements in practice means their "standard is now the sole viable foundation for a contact tracing app"); Reed Albergotti & Drew Harwell, *Apple and Google Are Building a Virus-Tracking System. Health Officials Say It Will Be Practically Useless*, WASH. POST (May 15, 2020, 3:22 PM), https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus (Apple and Google's announcement "sparked a wave of excitement" about potential to use to collect necessary information including location data).

[59] *See* JEFFREY KAHN ET AL., DIGITAL CONTACT TRACING FOR PANDEMIC RESPONSE 2 (Jeffrey Kahn ed., 2020) (recommending that apps provide users with "easy mechanisms and prompts to allow for opting-in to" providing location information); WORLD HEALTH ORGANIZATION, *CGU Digital Proximity Tracking Contact*, ETHICAL CONSIDERATIONS TO GUIDE THE USE OF DIGITAL PROXIMITY TRACKING TECHNOLOGIES FOR COVID-19 CONTACT TRACING, 3 (May 28, 2020) [hereinafter WHO], https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1 ("data collection should not require the identity or location data of a user, or a time stamp of a proximity event"); EUR. DATA PROT. BD., GUIDELINES 04/2020 ON THE USE OF LOCATION DATA AND CONTACT TRACING TOOLS IN THE CONTEXT OF THE COVID-19 OUTBREAK, 7 (Apr. 21, 2020) [hereinafter EDPB], https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf ("[C]ontact tracing apps do not require tracking the location of individual users. Instead, proximity data should be used.").

[60] *See* Jessica Rich, *How Our Outdated Privacy Laws Doomed Contact-Tracing Apps*, BROOKINGS INST.: TECHTANK (Jan. 28, 2021), https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps (arguing that "Americans just weren't persuaded" by Apple and Google's privacy measures); Mike Feibus, *Are Coronavirus Contact Tracing Apps Doomed to Fail in America?*, USA TODAY (June 24, 2020, 3:46 PM), http://www.usatoday.com/story/tech/columnist/2020/06/24/apple-google-contact-tracing-apps-privacy/3253088001.

[61] *See* Halper, *supra* note 55; *See Google Partner*, *supra* note 56.

companies incorporated the Bluetooth function into an operating system update, it caused alarm among many of their customers and prompted a widespread rumor that the companies secretly installed a "COVID-19 sensor" on their phones.[62]

Rather than praising the privacy-above-all approach of the Google-Apple system, press accounts and analyses by privacy advocates often described the system as posing substantial risks.[63] As late as September 2020, the Electronic Frontier Foundation criticized California legislators for considering adopting the Google-Apple system, warning them not to trust the tech giants' offer to create a pilot program free of charge because often services "offered for 'free' are paid for through the surrender of sensitive personal information."[64] In an ironic twist, many of those same analyses also cited the same technical constraints used to protect privacy—the unreliability of using Bluetooth, the need for large-scale adoption and the limits of exposure notification compared to traditional contact tracing—to argue that the system was unlikely to work.[65]

Second, Google's and Apple's announcements that they were limiting their systems to Bluetooth-based exposure notification effectively shut down any discussion of connecting digital contact tracing apps with other promising approaches to use multiple data sources in the pandemic response.[66] Early in the pandemic, many groups recommended using various information sources, including location information to help scale manual contact tracing. In April 2020, Johns Hopkins' Bloomberg School of Public Health and the Association

---

[62] *See*, *e.g.*, Feibus, *supra* note 60; David Murphy, *No, Your Phone Doesn't Have a 'COVID-19 Sensor,'* LIFEHACKER (Aug. 18, 2020, 10:00 AM), https://vitals.lifehacker.com/no-your-phone-doesnt-have-a-covid-19-sensor-1844750938; Rich DeMuro, *Yes, Coronavirus Tracking Was Installed on Your Phone. No, It's Not Doing Anything (Just Yet)*, KTLA5 (Jul. 3, 2020, 8:58 AM), https://ktla.com/morning-news/technology/covid-tracking-iphone-android-update.

[63] *See*, *e.g.*, ALBERT FOX CAHN & JOHN YANY VEISZLEMLEIN, STOP: SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, BEWARE: BLUETOOTH AHEAD 4–7 (2020) (critiquing Google-Apple system); Bennet Cyphers & Gennie Gebhart, *Apple and Google's COVID-19 Exposure Notification API: Questions and Answers*, ELEC. FRONTIER FOUND. (Apr. 28, 2020), (available at https://www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answersanswers) (listing privacy concerns and questioning whether the system will work).

[64] Hayley Tsukuyama, *California Still Needs Privacy Protections for COVID Tracking Apps*, ELEC. FRONTIER FOUND. (Sept. 9, 2020), https://www.eff.org/deeplinks/2020/09/california-still-needs-privacy-protections-covid-tracking-apps.

[65] *See, e.g.*, CAHN & VEISZLEMLEIN, *supra* note 63, at 7–9; Cyphers and Gebhart, *supra* note 63.

[66] *See*, *e.g.*, *Project Aurora: A New Open Source Solution for the Google Apple Exposure Notification API*, PATHCHECK FOUND. BLOG (May 20, 2020), https://www.pathcheck.org/en/blog/a-new-open-source-solution-for-the-google-apple-exposure-notification-api.

of State and Territorial Health Officials issued a joint report that called for using mobile contact tracing applications to collect contacts, location and self-reported symptoms.[67] That same month the Center for American Progress issued a comprehensive national and state plan for coronavirus response that recommended adopting tools for instantaneous contact tracing similar to South Korea's and Singapore's, which used "GPS, Bluetooth, cell tower and Wi-Fi networks" but with stronger protections for civil liberties.[68]

In May 2020, another research group issued a comprehensive set of recommendations for digital contact tracing. These recommendations emphasized that contact tracing apps should incorporate flexible design principles to allow for collection of new information as our understanding of the disease evolves and to permit users to opt into providing location information.[69]

Harvard's Edmond J. Safra Center for Ethics likewise noted that groups developing apps were increasingly moving toward incorporating a common Bluetooth architecture as the backbone for apps with a range of functions that would send "other information (such as personal information and GPS data)" to public health authorities.[70] In a similar vein, dozens of engineers, executives and epidemiologists issued an open letter calling on a range of technology companies to do more to address the pandemic. One of their thirteen recommendations was that Apple and Google should provide a privacy-preserving operating system function for contact tracing that included location information.[71] Citing the success of China and South Korea in conducting large-scale tracing, they called for the feature to allow users who opt in to determine if they had been in the same locations as subsequently identified cases.[72]

---

[67] CRYSTAL WATSON ET AL., JOHNS HOPKINS BLOOMBERG SCH. OF PUB. HEALTH: CTR. FOR HEALTH SEC., A NATIONAL PLAN TO ENABLE COMPREHENSIVE COVID-19 CASE FINDING AND CONTACT TRACING IN THE US 6 (2020), https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf.

[68] Zeke Emanuel et al., *A National and State Plan To End the Coronavirus Crisis*, CENTER FOR AMERICAN PROGRESS (Apr. 3, 2020), https://www.americanprogress.org/issues/healthcare/news/2020/04/03/482613/national-state-plan-end-coronavirus-crisis.

[69] KAHN ET AL., *supra* note 59, at 2–3, 7–10.

[70] VI HART ET AL., OUTPACING THE VIRUS: DIGITAL RESPONSE TO CONTAINING THE SPREAD OF COVID-19 WHILE MITIGATING PRIVACY RISKS, EDMOND J. SAFRA CTR. FOR ETHICS 23 (Apr. 3, 2020), https://ethics.harvard.edu/outpacing-virus.

[71] Peter Eckersley et al., *13 Things Tech Companies Can Do To Fight Coronavirus: An Open Letter From Technologists, Epidemiologists & Medical Professionals*, TECH VS COVID-19 (Apr. 2020), https://stop-covid.tech.

[72] *Id.*

The ACLU issued a set of recommendations for how policymakers should evaluate the potential use of tracking technologies to combat the epidemic. While emphasizing the need for caution, the report acknowledged that "[t]he challenges posed by COVID-19 are extraordinary, and we should consider with an open mind any and all measures that might help contain the virus consistent with our fundamental principles."[73] Specifically, under the right circumstances and with appropriate protections, "using certain forms of data generated by cell phones—such as location histories or records of proximity to other devices—might make sense."[74]

Third, Google's and Apple's requirements that each jurisdiction sponsor a single app, as well as the aggressive pressure they placed on governments already moving forward with alternatives to abandon those systems in favor of theirs, while intended to encourage user adoption, may have had the opposite effect. Most of the dominant network-dependent apps widely used today launched in small communities, developed broad adoption in those communities, and scaled from there.[75] Many of the groups developing alternative approaches were planning to pilot their apps in precisely that way both to test and refine how they work and to generate trust within local communities.[76]

Finally, a lesser-noticed but even more troubling aspect of Google's and Apple's approaches is the startlingly comprehensive control they were able to exert over public health responses across the world.[77] They

---

[73] JAY STANLEY & JENNIFER STISA GRANICK, ACLU, THE LIMITS OF LOCATION TRACKING IN AN EPIDEMIC 1 (Apr. 8, 2020), https://www.aclu.org/report/aclu-white-paper-limits-location-tracking-epidemic?redirect=aclu-white-paper-limits-location-tracking-epidemic.

[74] *Id.*

[75] *See* Chiara Farronato et al., *How To Get People to Actually Use Contact-Tracing Apps*, HARV. BUS. REV. (July 15, 2020), https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps.

[76] For example, the ShareTrace group that I worked with submitted a proposal to the National Institutes of Health proposing to pilot the app in one Northeast Ohio suburb and had started discussions with two local universities and one large health organization. Safe Paths had agreements with several local governments and non-profits to pilot their app. *See, e.g.*, Brian Kanerline, *KC Business Leaders, Companies Lead EBusiness Leaders, Companies Lead Effort to do Widespread COVID Contact Tracing*, KAN. CITY BUS. J. (May 9, 2020), https://www.bizjournals.com/kansascity/news/2020/05/09/executives-companies-lead-contact-tracing-effort.html (describing coalition of community groups "putting together a campaign to sell the public on using the Safe Paths app").

[77] Among the few commentaries that have highlighted this issue to date include Tamar Sharon, *Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers*, ETHICS & INFO. TECH. (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7368642.

forced several governments, including France, Germany, and the UK, to abandon their plans for digital contact tracing in favor of the limited Google-Apple system.[78] Many of these governments planned to pilot different designs with alternative approaches to privacy.[79] Even observers who generally approved of the Google-Apple system's privacy protections expressed dismay at the companies' brazen assertion of monopolistic power to dictate public health responses to the pandemic.[80]

IV. PANDEMIC PRIVACY

A. *Context*

Privacy depends on context.[81] Here that context starts with a highly infectious, often deadly disease that has killed millions of people, closed schools and universities, and wrought massive economic damage. In the U.S., common law rules and privacy laws have treated communicable diseases like COVID-19 as a special circumstance that justifies entrusting health authorities with rights to use sensitive data to protect the public.[82] Many jurisdictions even affirmatively require—

---

[78] *See* Alex Webb, *Apple and Google Face Off Against Europe Over Contact Tracing*, BLOOMBERG BUS. WEEK (May 18, 2020, 12:01 AM), www.bloomberg.com/news/articles/2020-05-18/apple-and-google-face-off-against-europe-over-contact-tracing; Douglas Busvine & Andreas Rinke, *Germany Flips to Apple-Google Approach on Smartphone Contact Tracing*, REUTERS (Apr. 26, 2020, 3:51 AM), www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J; Leo Kelion, *Coronavirus: Apple and France in Stand-Off Over Contact-Tracing App*, BBC NEWS (Apr. 21, 2020), https://www.bbc.com/news/technology-52366129.

[79] *See* Ieva Ilves*, Why Are Google and Apple Dictating How European Democracies Fight Coronavirus?*, THE GUARDIAN (June 16, 2020, 4:00 PM), https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus.

[80] *See, e.g.*, *id.*; Michael Veale, *Privacy is Not the Problem with the Apple-Google Contact-Tracing Toolkit*, THE GUARDIAN (July 1, 2020, 2:00 PM), https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights.

[81] *See, e.g.*, Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004). Nissenbaum applies this framework specifically to digital contact tracing tools in her presentation at Simons Institute, *Perspectives on Digital Contact Tracing*, YOUTUBE (July 20, 2020), https://www.youtube.com/watch?v=9J3s4h80Kxw. Nissenbaum argues that the Google-Apple system prioritized privacy at the expense of legitimate public health objectives. *Id.* at 38:00–41:25 min.

[82] *See, e.g.*, Polly J. Price, *Ebola and the Law in the United States: A Short Guide to Public Health Authority and Practical Limits* 5–13 (Emory Univ. Sch. of L. Res. Paper Series, Research Paper No. 14-299, 2015) (available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2538187) (describing state and federal laws and application to Ebola); *State Quarantine and Isolation Statutes*, NAT'L CONF. OF ST. LEGISLATURES (Aug. 7, 2020), https://www.ncsl.org/research/health/state-quarantine-and-isolation-

under the threat of civil or criminal penalties—that health care professionals and patients notify others who may be at risk of contracting a communicable disease.[83] Likewise, state and federal laws long have provided health authorities with extraordinary information-gathering powers to combat infectious disease, including repurposing consumer data collection methods like grocery loyalty cards and even credit card records to identify individuals at risk of contracting deadly diseases.[84]

The context also includes longstanding norms and practices related to the inherently intrusive manual contact tracing process.[85] That process involves collecting private and often sensitive information to identify every location a patient may have visited and every person he or she may have come into close contact with over the roughly two-week period when the patient likely was infectious. Standardized disease reporting guidance provides that for suspected COVID-19 cases, health authorities should gather and report, among other things, patient demographics, detailed symptoms, and all known contacts or linkages to COVID-19 cases.[86] To collect this information, contact tracers ask infected people detailed questions about where they have been and who they have met while they were contagious to identify other potential cases quickly.[87]

To assist in containing deadly diseases, health authorities routinely use multiple data sources outside of manual contact tracing, including individual consumer data. The Centers for Disease Control and Prevention (CDC)'s website on foodborne illness explicitly calls on health authorities and food companies to use information from

---

statutes.aspx; DANIELLE ALLEN ET AL., SECURING JUSTICE, HEALTH AND DEMOCRACY AGAINST THE COVID-19 THREAT, EDMOND J. SAFRA CTR. FOR ETHICS 11–17 (Mar. 24, 2020), https://drive.google.com/file/d/18ZEiscW_zHgyEn3-k_U2IJj7UgDhbi84/view.

[83] *See HIV and STD Criminalization Laws*, CTRS. FOR DISEASE CONTROL AND PREVENTION, https://www.cdc.gov/hiv/policies/law/states/exposure.html.

[84] *Safer Food Saves Lives*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Nov. 3, 2015) [hereinafter *Safer Food Saves Lives*], https://bit.ly/3d8Wjnt; *see* Frederik T. Moller et al., *Analysis of Consumer Food Purchase Data Used for Outbreak Investigations, A Review*, 23 EURO SUREVILLANCE, 1 (2018), https://pubmed.ncbi.nlm.nih.gov/29921346.

[85] For an extensive analysis of the public health needs that digital contact tracing could assist in meeting, see KAHN ET AL., *supra* note 59, at 13–14.

[86] COUNCIL OF ST. AND TERRITORIAL EPIDEMIOLOGISTS, POSITION STATEMENT NO. INTERIM-20-ID-02, UPDATE TO THE STANDARDIZED SURVEILLANCE CASE DEFINITION AND NATIONAL NOTIFICATION FOR 2019 NOVEL CORONAVIRUS DISEASE (COVID-19) (2020), https://cdn.ymaws.com/www.cste.org/resource/resmgr/ps/positionstatement2020/Interim-20-ID-02_COVID-19.pdf.

[87] *Investigating a COVID-19 Case*, CTRS. FOR DISEASE CONTROL AND PREVENTION (Nov. 23, 2020), https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/investigating-covid-19-case.html.

individual grocery loyalty cards to identify potential sources of confirmed salmonella and to notify other individuals who are at risk from consuming the same contaminated product.[88] Likewise, the CDC's detailed contact tracing guidelines for COVID-19 list "Google maps" and "social media/mobile apps" as recommended alternative sources of information to identify close contacts.[89]

These general public health norms for communicable disease and the specific practices related to contact tracing, including the types of information collected, establish the context in which we should consider the privacy implications of digital tools to accomplish the same ends.[90] Discussing privacy in light of this context and taking into account the potential for digital health surveillance tools to slow the spread of disease appropriately recognizes both the risks and benefits of deploying them.

B. *Google-Apple Exposure Notification and Safe Paths Privacy Comparison*

The key questions, then, are: (i) what new privacy risks do digital contact tracing tools pose compared to the information that health authorities already collect and (ii) are those risks acceptable in light of the potential benefits? Comparing the potential risks and benefits of the Bluetooth-only Google-Apple system and the Safe Paths GPS-plus Bluetooth proposal in light of the context just described illustrates how one alternative to the dominant Apple-Google model could have increased the efficacy of digital contact tracing with very little increase in privacy risk to individual users.

The Google-Apple system collects far less sensitive information than manual contact tracing. The system records only rotating, anonymous identifiers and destroys those identifiers after fourteen days. These identifiers stay on a user's device until the user tests positive and consents to upload them to a central server controlled by a public health authority to alert other users who may have been exposed.

---

88 *Safer Food Saves Lives*, *supra* note 84.

89 *Case Investigation and Contact-Tracing Guidance*, CTRS. FOR DISEASE CONTROL AND PREVENTION, Appendix B (Nov. 23, 2020), https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/contact-tracing-plan/appendix.html#tips.

90 For an extended analysis of these issues from an ethics perspective see Michael J. Parker et al., *Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the Control of the COVID-19 Pandemic*, 46 J. MED. ETHICS 427–31 (2020), https://jme.bmj.com/content/medethics/46/7/427.full.pdf.

It is difficult, but not impossible, to re-identify an individual using those rotating identifiers.[91] For example, a person with a Bluetooth-enabled camera could use that device to capture identifiers broadcast by individuals in a specific location and simultaneously "root" their phone, which is running the app to let them see the Bluetooth identifiers of other users the camera is recording. If one of those users later reports a positive COVID-19 diagnosis, the person doing the recording could match up the codes the user broadcast at the moment they passed the camera, identifying a stranger as COVID-19 positive.[92]

This risk is real, but it is difficult to execute and impossible to scale. The camera attack is far less likely to identify someone than alternatives like directly surveilling known COVID-19 testing sites. More importantly, the privacy risk it creates is minimal compared to the information routinely collected as part of manual contact tracing.

The problem is that the Google-Apple system completely ignores the public health context in favor of protecting user privacy. As one public health expert put it, the Google-Apple system "took out the most important piece, which was the location of where people were."[93] Rather than addressing the specific needs of public health authorities in contact tracing and other processes, the system's only potential value lies in its ability to alert some people with access to the right kind of device that they may have been exposed to an infected person.[94] Even that potential requires relatively high adoption rates among the subset of people with phones capable of using the system and is subject to relatively high risk of false positives.

The Safe Paths app proposed a system designed to interface directly with public health systems and processes, including manual contact tracing, using that same Bluetooth protocol and adding GPS

---

[91] For a summary of the technical details regarding these risks see Russell Brandon, *Answering the 12 Biggest Questions About Apple and Google's New Coronavirus Tracking Project*, THE VERGE (Apr. 11, 2020, 10:48 AM), https://www.theverge.com/2020/4/11/21216803/apple-google-coronavirus-tracking-app-covid-bluetooth-secure.

[92] *See id.*; Andy Greenberg, *Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered*, WIRED (Apr. 17, 2020, 7:00 AM), https://bit.ly/3f1YICI.

[93] Margaret Bourdeaux, *Covid State of Play: Building a Public Sector Health Intelligence Capability*, Berkman Klein Ctr. for Internet & Soc'y (Dec. 16, 2020), https://cyber.harvard.edu/events/covid-state-play-building-public-sector-health-intelligence-capability.

[94] For discussions of the need for apps to interface with public health authorities, see Margaret Boudreaux, et al., *The Best Tech for Contact Tracing? Systems Designed for Healthcare Workers*, 9 Interactions XXVII.4, 90 (July–Aug. 2020); *see also*, Nissenbaum, *supra* note 81, at 120.

location information and time.[95] In the abstract, these additional pieces of information pose substantially more privacy risks than the Google-Apple system because even a fourteen-day location history reveals sensitive details about a person to the health authority collecting that information. But manual contact tracing collects that same information, and the privacy protections Safe Paths incorporates arguably better protects this information than that process.[96]

Safe Paths poses two additional risks. First, a person only provides location information in the manual contact tracing process after they have tested positive, whereas the Safe Paths app routinely collects and stores fourteen days of contacts. Collecting and storing those contacts opens up users to the risk that someone could access those contacts at any time. Second, users risk reidentification where health authorities use the de-identified and aggregated location to publish public heat maps that allow non-users to self-identify possible exposure.[97]

Safe Paths includes several protections to mitigate both of those additional risks. First, Safe Paths uses the same decentralized structure as the Google-Apple system storing both Bluetooth keys and location information directly on the user's phone. The system also proposed several alternatives for protecting sensitive GPS information from unauthorized access or reidentification.[98] This combination of measures provides users complete control over the information the app collects; thus, minimizing any privacy risk during the collection process itself. Notably, they also provide greater protections than many popular consumer applications that track location, including Google and Apple maps.[99] Second, the Safe Places system allows health authorities to

---

[95] *See, e.g.*, Ananthaswamy, *supra* note 40; Raskar, *Apps Gone Rogue*, *supra* note 35; *Covid SafePaths*, *supra* note 19, at 20–23 (emphasizing need for apps to work with public health authorities and describing benefits of that collaboration).

[96] *See* Alex Berke et al., *Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy*, MIT MEDIA LAB, Mar. 31, 2020, at 6–9, https://arxiv.org/pdf/2003.14412.pdf; *see also* Ananthaswamy, *supra* note 40.

[97] *See Adding Location Context*, *supra* note 21 (describing threats and identifying solutions).

[98] *See* PATHCHECK, "GPS+ Solution," PATHCHECK FOUNDATION [hereinafter GPS+], https://www.pathcheck.org/en/technology/gps-digital-contact-tracing-solution; Raskar, *Apps Gone Rogue*, *supra* note 35, at 6. Safe Paths proposed several alternatives for storing the GPS information, including: (1) logging direct GPS information but without visualization to prevent casual unauthorized access by nosy co-workers, spouses or employers; or (2) "blurring" GPS information based on population density and storing only that less precise location also without visualization. It also requires users affirmatively to consent to upload that information to a public health authority-maintained server. *See Adding Location Context*, *supra* note 21.

[99] *See* ME AND MY SHADOW, *Location Tracking*, (Feb. 15, 2017), https://myshadow.org/location-tracking.

redact any location that a user does not want included in the aggregated database. It also is set up to delete the raw individual data and to aggregate that de-identified information.[100]

In spite of these protections, by allowing users to provide raw location information directly to a public health authority the Safe Paths app poses a more significant privacy risk to users than the Google-Apple app. Using the app to collect this information, however, does not substantially increase the risk that manual contact tracing poses because a user provides location information to health authorities through that process. Once the raw data is destroyed through Safe Places, no new personal information is retained.

The concern most often identified over collecting location information with these apps is the risk of surveillance creep. Safe Paths' decentralized structure largely eliminates that concern. Rather than creating a new large-scale centralized database, the Safe Paths system stores that information on users' phones. Law enforcement authorities still could seek to access the records of individuals who test positive and share their stored location data with health authorities. The Safe Places system accounts for that risk by providing tools for health authorities to delete the raw data after it is de-identified and aggregated with other users.

While it is certainly possible with some additional information to connect an individual to one or more specific locations, it would be difficult to use the aggregated data to recreate a single person's location history or do anything else that is likely to provide useful information in a law enforcement investigation.[101] It would be much easier to gather the same and much more information from other sources, including manual contact tracing databases, which maintain records connected to each individual. Indeed, as Stewart Baker wryly observed "any authoritarian government worth its salt could get far more location and contact data simply by subpoenaing Google's adtech files" than it could even from a digital contact tracing database that stored location records connected to each person, much less one like Safe Paths that stores only aggregated data.[102]

---

100 *See* GPS+, *supra* note 98; PathCheck Github, *supra* note 37.

101 *See*, *e.g.*, Alsdurf et al., *supra* note 33, at 17–20 (describing in detail reidentification and other threats for decentralized contact tracing).

102 Stewart Baker, *The Problem With Google and Apple's COVID-19-Tracking Plan*, LAWFARE, (Apr. 14, 2020), https://www.lawfareblog.com/problem-google-and-apples-covid-19-tracking-plan. Indeed, Google and several ad tech companies that aggregate location data already shares that information with public health officials and researchers as part of their coronavirus response efforts. *See* GOOGLE, *COVID-19 Community Mobility Reports*, https://www.google.com/covid19/mobility/; PRIVACY

The point in analyzing Safe Paths closely is not to argue that it was the best model for digital contact tracing. Indeed, there was an active debate over whether the privacy benefits of a largely decentralized model system were worth the efficiency and efficacy tradeoffs.[103] The Safe Paths example simply illustrates that Google's and Apple's decisions to impose a single privacy model cut off even highly privacy protective but still potentially more useful alternatives. It also ended the progress they were making to pilot and test those options with several communities.

The next Section first explains how adding only location information with the privacy protections Safe Paths incorporated could have been more effective than the Google-Apple model. It then explores how other types of information have the potential to make these apps even more powerful tools and how some of that information is critical to evaluating whether these tools are working and how they are affecting different communities. Here, again, the claim is not that any of these possibilities definitively would have worked, only that the rush to install a single, uniformly limited design prevented even responsible experimentation with them.

C. *Efficacy and Effectiveness*

Health researchers carefully distinguish between the efficacy and effectiveness of new interventions.[104] Efficacy reflects how well an intervention works under controlled, ideal conditions whereas effectiveness measures its performance in the real world.[105] Critiques of the efficacy of digital contact tracing apps typically focus on the Google-Apple system and often involve a catch-22: they start with assuming (or insisting on) the set of privacy controls those companies have imposed to radically limit the information the apps can collect and

---

INTERNATIONAL, *US State and Local Authorities Strike Deals With Location Data Companies*, (June 15, 2020), https://privacyinternational.org/examples/4008/us-state-and-local-authorities-strike-deals-location-data-companies (noting that "Apple's and Google's refusal to allow contact tracing apps using their system to access location services on users' phones creates an opportunity for these data providers").

[103] *See* Joseph Duball, *Centralized vs. Decentralized: EU's Contact Tracing Privacy Conundrum*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Apr. 28, 2020), https://iapp.org/news/a/centralized-vs-decentralized-eus-contact-tracing-privacy-conundrum.

[104] *See* Amit G. Singal et al., *A Primer on Effectiveness and Efficacy Trials*, 5 CLINICAL AND TRANSLATIONAL GASTROENTEROLOGY 1 (2014).

[105] *Id.* at 1.

what health authorities can do with it and then conclude that this tightly handcuffed system is unlikely to work.[106]

Recent studies have used proxies to estimate that even apps using the extremely limited Google-Apple system are working better than critics predicted.[107] The Safe Paths example illustrates how incorporating even modest additional information into digital contact tracing applications increases their efficacy in combating the pandemic by making them useful to public health authorities as well as users in several ways.[108] The ability to collect even that modest but critical location information would allow us to test the system's effectiveness and tailor it to work better in future iterations. Collecting modest additional information, including demographic information, would allow analyses of whether and how the app is helping or harming specific communities, including those hit hardest by the disease.[109]

Contrary to what several analyses assert, combining location data with Bluetooth is far more useful than relying solely on Bluetooth.[110] First, it allows for more accurate assessments of exposure.[111] Second,

---

[106] *See, e.g.*, Ashkan Soltani et al., *Contact-Tracing Apps Are Not a Solution to the COVID-19 Crisis*, BROOKINGS TECH STREAM (Apr. 27, 2020), https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster (critiquing the Google-Apple system).

[107] *See* Malcolm Owen, *UK Apple-Google COVID-19 App Credited for Prevention of 600,000 Infections*, APPLEINSIDER, (Feb. 9, 2021), https://appleinsider.com/articles/21/02/09/uk-apple-google-covid-19-app-credited-for-prevention-of-600000-infections.

[108] *See* Ramesh Raskar et al., *Contact Tracing: Holistic Solution Beyond Bluetooth*, https://github.com/PrivateKit/PrivacyDocuments/blob/master/ContactTracingBeyondBluetooth.pdf; COVID SAFE PATHS, *COVID-19 Contact-Tracing Mobile Apps: Evaluation and Assessment for Decisionmakers*, https://github.com/PrivateKit/PrivacyDocuments/blob/master/apps-evaluation.pdf; Maria Barsallo Lynch & Lauren Zabierek, *Considerations for Digital Contact Tracing Tools for COVID-19 Mitigation: Recommendations for Stakeholders and Policymakers*, BELFER CTR. FOR SCI. AND INT'L AFF. 15 (June 2020), https://www.belfercenter.org/publication/considerations-digital-contact-tracing-tools-covid-19-mitigation-recommendations#toc-3-3-0 (noting that Bluetooth exposure notification and location services "may complement each other and yield a more effective solution for contact tracing," but the Google-Apple system prohibits it).

[109] *See* Anasthswamy, *supra* note 40.

[110] Margaret Bourdeaux put this most succinctly when she noted that "[Google and Apple] took out the most important piece, which was the location of where people were." Bourdeaux, *supra* note 93; *see also* KAHN ET AL., *supra* note 59, at 2 (recommending that contact tracing apps permit users to opt into location tracking). For examples of analyses stating that location data is unnecessary see WHO, *supra* note 59 and EDPB, *supra* note 59.

[111] *See Holistic Solution*, *supra* note 19; Nancy A. Fairbank et al., *There's an App for That: Digital Contact Tracing and Its Role in Mitigating a Second Wave*, at 13–14, https://cyber.harvard.edu/sites/default/files/2020-05/Contact_Tracing_Report_Final.pdf; Kostubh "K.J." Bhagchi et al., *Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns*, Edmond J.

an app that collects location information requires lower adoption rates for the app to work.[112] Finally, it makes the apps directly useful for traditional contact tracing and provides information that health authorities could aggregate and use to better target scarce resources and refine their understanding of how the disease spreads and who is most at risk.[113]

One of the most significant hurdles for any app is adoption rate. Several surveys have shown a marked reluctance among Americans to use these apps.[114] Privacy concerns clearly play a substantial role in this reluctance, but at least one study suggests that in the U.S. people are somewhat more concerned with an app's effectiveness than with privacy, although both issues were likely to result in lower adoption rates.[115] It makes sense that the public is more likely to trust and use a more robust tool that is more accurate and effective while still protecting user privacy.

Equally important, adding location and other information, such as symptoms and health data, could make these apps useful at much lower adoption rates for several reasons. First, a system like Safe Paths could be used to assist in manual contact tracing and for the other functions like identifying emerging hotspots.[116] Second, these functions also make the apps useful for a much larger range of people, including those with older phones unable to use the Google-Apple system.[117]

Beyond identifying individual cases, health officials have used machine learning and other data analytics tools to trace the source or model the likely future spread of infectious diseases.[118] These tools are especially valuable for outbreaks caused by new diseases, like COVID-19, where we lack information about how the disease spreads and what factors put individuals at risk.[119] Critically, these data analytics tools

---

Safra Center for Ethics, COVID-19 Rapid Response Initiative White Paper 22, July 2, 2020, at 11–12.

112 *See Holistic Solution*, *supra* note 19.

113 *See* Bourdeaux, *supra* note 93, Podcast Transcript at 7–9.

114 *See* Kaptchuk et al., *supra* note 30.

115 *Id.*

116 *See id.*; *Holistic Solution*, *supra* note 19.

117 *See* Alex Berke et al., *Assessing Disease Exposure Risk with Location Data: A Proposal for Cryptographic Preservation of Privacy*, MIT MEDIA LAB, Mar. 2020, at 3.

118 *See* Zheng et al., *Artificial Intelligence–Enabled Public Health Surveillance—from Local Detection to Global Epidemic Monitoring and Control*, Art. Intell. *in* Med. 437 (2021), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7484813.

119 *See* Bourdeaux, *supra* note 93, at 7–8, ("Relying on digital data sources, such as data from mobile phones and other digital devices, is of particular value in outbreaks caused by newly discovered pathogens, for which official data and reliable forecasts are still scarce."); Marcello Ienca and Effy Vayena, *On The Responsible Use of Digital Data to*

have been used in the current pandemic to help triage allocation of scarce resources to vulnerable communities most at risk from the disease.

As one data science expert explained recently, combining contact tracing-related apps with these powerful analytic tools could make them valuable well beyond alerting users about their own potential exposure.[120] This is because tracking apps can provide the granular, real-time information about who is contracting the disease, where they live, and what symptoms they are experiencing; these advanced tools need to more quickly and precisely identify how the disease spreads, especially among people and communities at higher risk.[121] That same information could improve pandemic response in a range of other ways, including quickly tracking the real-time effects of different policy decisions like re-opening schools and restaurants.[122] These potential applications, when combined with statistical modeling, also require much lower adoption rates to work.[123]

Integrating these apps with data provided by other tools like mobile fitness apps creates even more potential for this kind of synergistic analysis. The health wearable studies cited at the beginning of this Article show the tremendous potential for repurposing the information existing devices already collect.[124] Notably, both studies demonstrated that aggregating information allowed for much faster diagnoses even in asymptomatic patients.[125] This provides a potential solution to the problem of testing shortages by offering an alternative. Adding location information could make the notifications even more accurate by reducing the number of false positives for individuals.

Layering additional information also has the potential to refine our understanding of when a person who has contracted the disease safely can return to work or school. One study found that using what the researchers call risk-based quarantine—essentially incorporating symptom monitoring for individuals with a common exposure source

---

Tackle the COVID-19 Pandemic, 26 NATURE MED. 463, 463 (2020), available at https://www.nature.com/articles/s41591-020-0832-5.

120 Kimon Drakopoulos, *The Logic Around Contact Tracing Apps Is All Wrong*, WIRED (Aug. 13, 2020). https://www.wired.com/story/opinion-the-logic-around-contact-tracing-apps-is-all-wrong/.

121 *See* Andrew Curtis et al., *Geographic Monitoring for Early Disease Detection (GeoMEDD)*, NATURE SCIENTIFIC REPORTS 10 (2020), https://www.nature.com/articles/s41598-020-78704-5.pdf.

122 *Id.*

123 *Id.*

124 *See supra* Part I.

125 *See* Hirten et al., *supra* note 1; Mishra et al., *supra* note 2.

into manual contact tracing—is potentially more effective than single-test release protocols.[126] Another study found that using a mobile self-reporting symptom tracking app predicted the emergence of new hotspots five to seven days earlier than relying on public health reports.[127]

These broader possibilities for using data collected through these apps and other tools to better understand this disease and identify more effective responses outside of simple tracking and tracing highlights the costs of applying a one-size-fits-all set of privacy controls to them. Several recent studies have concluded that the use of more robust digital surveillance tools in other countries has both saved lives and mitigated the devastating economic effects of the pandemic. One retrospective comparison of six countries' different use of digital tools as part of their pandemic response efforts concluded that "early intervention with the use of digital tools had a strong correlation with the successful containment of COVID-19."[128] Likewise, a National Bureau of Economic Research study of South Korea's broad-based use of digital tools found the tools likely saved thousands of lives and substantially mitigated the economic effects of the pandemic by avoiding costly lockdowns.[129] A similar study of China's extensive use of mobile-phone location data reached similar conclusions.[130]

The point of citing those studies is not to argue that the pandemic justifies wholesale adoption of these more intrusive measures. Indeed, the protections Part V outlines would preclude many of them. Rather, these studies suggest that allowing apps to collect—and health authorities to use—more information than mere Bluetooth proximity data could make these apps more useful.[131]

Notably, some of the apps using the Google-Apple system have implicitly recognized these benefits by finding ways to incorporate some limited additional data within the tight restrictions these

---

126 Andrew Perrault et al., *Designing Efficient Contact Tracing Through Risk-Based Quarantining* 14 (Nat'l Bureau of Econ. Research, Working Paper No. 28135, 2020).

127 David A. Drew et al., *Rapid Implementation of Mobile Technology for Real-Time Epidemiology of COVID-19, Science*, 368 SCIENCE 1362, 1366 (2020), https://science.sciencemag.org/content/368/6497/1362/tab-pdf.

128 Kylie Zeng et al., *The Use of Digital Tools to Mitigate the COVID-19 Pandemic: Comparative Retrospective Study of Six Countries*, 6 JMIR PUB. HEALTH SURVEILL. 4, 4 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7759507/?report=printable.

129 David O. Argente et al., *The Cost of Privacy: Welfare Effects of the Disclosure of COVID-19 Cases,* NBER Working Paper 27220, available at, https://www.nber.org/system/files/working_papers/w27220/w27220.pdf

130 Kairong Xiao, *The Value of Big Data in a Pandemic*, Manuscript at 2, 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3583919.

131 *See* Bourdeaux, *supra* note 93.

companies have imposed. For example, the UK app has added two limited forms of location information. First, users are required to input their postcode and identify their local authority when registering to allow local authorities to provide specific advice and support, and also to permit analysis of the app's effectiveness.[132]

Second, the app has incorporated an indirect form of location tracking by allowing users to scan official QR codes posted on some public venues and store those codes on the device for 21 days.[133] The app does this for precisely the same reasons that Safe Paths proposed permitting users to store their own location data but in a far more cumbersome and less effective way. Rather than allowing users to take advantage of the same location logging functions they already often use to provide that information to consumer apps, the system requires them to remember to look for QR codes in places they visit and then physically scan those codes with their phones.

It also appears that, rather than integrating this with the Bluetooth keys to create an integrated risk score as Safe Paths and others proposed, this function operates in parallel so that users who opt into both may receive separate proximity alerts and venue-based alerts.[134] Public health authorities and researchers also cannot access this information to refine the system or better understand the disease. Instead, they are left attempting to draw indirect inferences even for very basic data points that direct location logging easily could provide.[135]

By creating an interoperable design standard for Bluetooth exposure notification, Google and Apple could have facilitated the development of these more powerful alternatives. Indeed, many people involved in developing apps applauded their announcement as an

---

132 *See* UK Dept. of Health & Social Care, *NHS COVID-19 App: Data Protection Impact Assessment*, GOV.UK (Feb. 11, 2021), https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment (describing all of the app's functions, including "addition of local authorities," and reasons for these new functions).

133 *Id.*; *see also* Briers, et al., *supra* note 32 (explaining that the QR code "feature allows health officials to send venue alerts and advice to users, and for users to keep a private and secure digital log of the places that they have visited, should they ever need to report this information to contact tracers").

134 *See* UK Dept. of Health & Social Care, *supra* note 132.

135 *See* Briers et al., *supra* note 32. This report describes the very sophisticated tools researchers have used to attempt to assess how the system is working. In one particularly telling example, the researchers note that they "have just finished producing *preliminary research into the potential for a mobile device to infer whether an encounter takes place indoors or outdoors*. This information could help to inform the risk calculation, and potentially wider public policy." (emphasis added).

opportunity for the apps in development to work off a universal, interoperable core.[136] By strictly limiting apps using this tool from collecting any other information, Google and Apple effectively foreclosed the possibility of experimenting with both collecting different combinations of information, except in the highly attenuated ways the UK example illustrates, as well as alternative privacy models for protecting that information.

D. *Equity*

Beyond privacy and effectiveness, another important set of concerns with using smartphone apps is that they risk exacerbating the already deeply inequitable effects of the pandemic on marginalized communities.[137] To start, the Google-Apple system depends on owning an expensive smartphone and consistent internet access. Recent studies estimate that up to 2 billion of the 3.5 billion phones in use across the globe will be unable to use this system.[138]

Even for people with access to smartphones capable of running the Google-Apple system, the risk of a false positive notification is greater for many marginalized communities and the consequences potentially more severe for several reasons.[139] The disease is more widespread in these communities.[140] Racial minorities, and Black Americans in particular, are more likely to live in denser spaces, including apartments and multi-family units, and are overrepresented essential jobs with large numbers of interactions, including frontline healthcare workers, grocery stores, and fast-food restaurants.[141] The unnecessary quarantine that could result from a false positive also is more likely to

---

136 *See, e.g.*, SafePaths Alliance, *Adding Location Context to Apple/Google Exposure Notification Bluetooth API: MIT SafePaths Encryption Proposals for GPS + Bluetooth*, PATHCHECK FOUND. (May 5, 2020), https://www.pathcheck.org/en/blog/adding-location-context-to-apple-google-exposure-notification-bluetooth-api-mit-safepaths-encryption-proposals-for-gps-bluetooth; *ShareTrace*, *supra* note 33, at 4–5, 11.

137 *See* Delan Devakumar et al., *Racism and Discrimination in COVID-19 Responses*, 395 LANCET 1194, 1194 (2020).

138 Tim Bradshaw, *2 Billion Phones Cannot Use Google and Apple Contact-Tracing Tech*, ARS TECHNICA (April 20, 2020), https://arstechnica.com/tech-policy/2020/04/2-billion-phones-cannot-use-google-and-apple-contract-tracing-tech.

139 *See, e.g.*, Devakumar et al., *supra* note 137, at 1194; Susan Landau, et. al., *The Importance of Equity in Contact Tracing*, LAWFARE (May 1, 2020), https://www.lawfareblog.com/importance-equity-contact-tracing.

140 *See* Devakumar et al., *supra* note 137, at 1194.

141 *See* Adam Nagy, *What Digital Contact Tracing Can Teach Us About Public Trust, Health Equity, and Governance in the United States*, MEDIUM (Oct. 29, 2020), https://medium.com/berkman-klein-center/what-digital-contact-tracing-can-teach-us-about-public-trust-health-equity-and-governance-in-the-510ce5f2c6f6.

result in lost income or even firing for those in low-wage hourly jobs.[142] If use of an app is made mandatory for public or private services, the higher risk of false positives also could disproportionately deny access to these same groups.

Many of these issues require the kind of legal protections identified in Part V. Several of these problems, however, either are a direct result of the Google-Apple system's reliance solely on Bluetooth or exacerbated by its limits. First, as noted above, a system that relies on both GPS and Bluetooth proximity would be accessible to far more people. Google's and Apple's systems directly exclude people without access to newer phones. To make matters worse, because the system collects only Bluetooth information it does not even indirectly benefit non-users in the ways that location systems can.

Second, adding location information significantly reduces the risk of false positives that disproportionately harm low-income people and people of color.[143] More importantly, in contrast to the Google-Apple system, which is designed to minimize involvement of the public health system and actively prevent it from accessing any information from users, systems like Safe Paths are designed to interface directly with the manual contact tracing system.[144] Establishing this connection is critical to providing necessary support and resources and the extensive benefits of interacting with trained, caring health professionals.

Collecting more information is also critical for health authorities to better understand how the disease spreads, develop more effective risk mitigation strategies (including more refined quarantine recommendations), and more effectively allocate scarce resources to people at higher risk.[145] The Berkman Klein Center for Internet & Society Digital Pandemic Response Working Group identified as a major issue of concern the significant gaps in the data we need to understand the disparate impacts of this pandemic, in particular with respect to demographic information like race and ethnicity.[146] In the absence of this detailed demographic information doctors and epidemiologists have resorted to devising improvised tools for estimating the effects of

---

142 *Id.*

143 *See Holistic Solution*, *supra* note 19.

144 *Id.*

145 *See, e.g.*, Drew et. al., *supra* note 127, at 3–5 (describing mobile applications collecting symptoms and other information). For a much more extensive analysis of how digital technology, including apps, could be deployed to improve pandemic response, see Petar Radanliev, et al., *COVID-19 What Have We Learned? The Rise of Social Machines and Connected Devices in Pandemic Management Following the Concepts of Predictive, Preventive and Personalized Medicine*, 11 EPMA JOURNAL 311, 312 (2020).

146 Nagy *supra* note 141.

the pandemic on different groups and to identifying tailored response strategies.[147]

Third, by preventing apps using their system from collecting location and other information, these companies have made it impossible to conduct the kind of iterative equity analyses that are essential to assessing whether and how these apps are helping or harming marginalized groups.[148] The Google-Apple system's privacy protections make it difficult even to assess whether the app is working at all and impossible to analyze demographic differences.[149]

Having this kind of information is essential to configuring apps and designing complementary alternatives both to maximize access and ensure they benefit as many people as possible, as well as to minimize disproportionate harms on particular groups.[150] The problem with Google's and Apple's systems is that they have frozen into place a single design standard that both prevents us from understanding what works and prevents the kind of experimentation necessary to develop apps or combinations of apps that could work better for everyone.[151]

V. TRUSTWORTHY PANDEMIC PRIVACY

Effective disease surveillance does not have to give up on privacy. Most of the privacy threats digital contact tracing raises could be guarded against by strong and verifiable restrictions on how every person's data is accessed, used, and deleted while still allowing for broader use of potentially sensitive information, including location information. We can protect privacy and enable a more effective and equitable health surveillance system by putting in place a framework that collects only information necessary for public health, keeps

---

147 *See* Karthik Sivashanker et al., *A Data-Driven Approach to Addressing Racial Disparities in Health Care Outcomes*, HARV. BUS. REV. (July 21, 2020), https://hbr.org/2020/07/a-data-driven-approach-to-addressing-racial-disparities-in-health-care-outcomes.

148 *See, e.g.*, KAHN ET AL., *supra* note 59; Landau, *supra* note 139 (calling for developing apps through a process "designed to identify and address potential demographic disparities early and continuously").

149 *See* Chris Wymant et al., *The epidemiological impact of the NHS COVID-19 App*, https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Epidemiological_Impact_of_the_NHS_COVID_19_App_Public_Release_V1.pdf (describing complex indirect information necessary to estimate effects of UK app).

150 *See* KAHN ET AL., *supra* note 59.

151 *Id.*; *see also* Zak Doffman, *Yes, Apple And Google Have Given Us A Serious Contact Tracing Problem—Here's Why*, FORBES (Jun. 19, 2020, 5:17 AM), https://www.forbes.com/sites/zakdoffman/2020/06/19/how-apple-and-google-created-this-contact-tracing-disaster ("The rigid policing of a common framework has tied governments' hands around the world, offering no flexibility to adapt to scientific advice on these unprecedented solutions for the global pandemic.").

sensitive health data secure from redistribution or repurposing, transparently monitors how that data is used and assesses whether the program works and how it affects vulnerable communities.[152]

Much of the concern over digital contact tracing centers over the fear that any tool that routinely collects sensitive personal information, no matter how well intentioned, can too easily be repurposed for use by law enforcement to use in criminal investigations or the national security apparatus to spy on individuals. Those concerns are heightened for people of color who historically have been disproportionately disadvantaged by new surveillance and other digital tools.[153]

The public health context is very different from counterterrorism or law enforcement. The legitimate need to hide sources and methods makes meaningful transparency and effective oversight of national security surveillance programs extremely difficult. Public health, even during emergencies like the current pandemic, does not require similar secrecy. Disease surveillance programs can be monitored and audited, without disclosing personally identifying information, to ensure compliance with data access and purpose limitations.

Jane Bambauer and I have identified several core features of a national pandemic privacy law necessary to provide a uniform, transparent, legally enforceable set of protections to enable the responsible collection and use of information to protect public health in future pandemics.[154] These include setting up a national data repository that integrates information from digital contact tracing apps as well as other relevant sources. Congress, in the March 2020 CARES Act, required the CDC to develop data-driven COVID-19 solutions and appropriated $500 million to them for "public health data surveillance and analytics infrastructure modification."[155] President Biden's COVID-19 national strategy similarly calls for ramping up the federal government's collection, production, sharing and analysis of data to

---

[152] Several groups have recommended similar approaches with more detailed guidelines for implementing them even in the absence of formal legal protections. *See*, *e.g.*, KAHN ET AL., *supra* note 59; *see* Kelsey Finch et al., Digital Contact Tracing: A Playbook for Responsible Data Use, (Aug. 14, 2020), https://law.mit.edu/pub/digitalcontact tracingaplaybookforresponsibledatause/release/1.

[153] *See* Finch et al., *supra* note 152.

[154] *See* Bambauer & Ray, *supra* note 5.

[155] Daniel Felz et al., *BREAKING: Location and Mobile Data in the Fight against COVID-19—An Overview of U.S. and Global Efforts*, JD SUPRA (Apr. 13, 2020), https://www.jd supra.com/legalnews/breaking-location-and-mobile-data-in-47904/.

"support an equitable COVID-19 response and recovery."[156] Both initiatives could incorporate developing this kind of data repository.

The law should limit the data collection system to collecting only information that is necessary to protect public health. Any information that in itself or with other information, including location information should be de-identified and the raw data deleted as soon as possible. Access to the information should be strictly limited to public health authorities and any access to law enforcement should be prohibited.

Those use and access restrictions should be enforced through complete transparency about the system's design and use without disclosing any user data. The source code should be open to the public. The system should log every access to the data and make the access logs public. And the purpose of any non-routine access should also be logged. Routine audits should be conducted either by an independent agency or trusted third party.

Perhaps the most important privacy protection is ensuring that the data repository lasts only as long as the need for the program. The program should automatically expire when the emergency has ended or when an internal or independent review finds that the data surveillance has not added sufficient value for controlling the outbreak.

Some have questioned whether we need a stand-alone privacy law to protect the data collected during pandemics and instead call for incorporating those protections into a comprehensive consumer data privacy law.[157] While I am sympathetic to the idea of a comprehensive consumer data privacy law—and appreciate the irony inherent in establishing potentially greater privacy protections for the collection and use of information during public health crises than for routine consumer transactions—the public health context is very different from consumer privacy. Lack of careful thought about those differences and the tradeoffs we should be willing to make is a large reason we ended up with the ineffective apps that we have today.

A stand-alone pandemic privacy law is necessary to tailor these protections to the specific context of public health generally and pandemics specifically. Several of the protections we identified, including the automatic sunset clause, make sense only in the emergency context of a pandemic. Perhaps most importantly, we need

---

156 Kat Jercich, *Biden's COVID-19 Plan Depends on a Data-Driven Approach for Efficacy, Equity*, HEALTHCARE IT NEWS (Jan. 21, 2021), https://www.healthcareitnews.com/news/bidens-covid-19-plan-depends-data-driven-approach-efficacy-equity.

157 *E.g.*, Rich, *supra* note 60 ("[W]e need a baseline federal privacy law to establish clear and enforceable privacy rules across the entire marketplace, one that protects our personal information in good times and in times of crisis.").

a pandemic privacy law with the protections just described not merely (and not primarily) to protect the privacy of the information the system collects. We need a law that will enable public health authorities to collaborate with technology developers to develop, test, and refine new tools to understand and respond to new diseases like COVID-19 quickly and to ensure that those tools address rather than exacerbate existing inequalities.[158]

Our original set of minimum principles left out this key requirement: the law should require that the system collect the information necessary to determine whether new digital tools serve public health needs and how they affect different groups, especially those most at risk. We recommended that authorization to create the data repository should include an independent oversight board to monitor administration of the program. In addition to ensuring that the information is not used for any purpose other than public health as we originally proposed, this board should be required to partner with outside experts to design and conduct iterative studies of whether and how digital contact tracing methods are assisting in the public health response and how they can be improved.[159] These studies should include specific analysis of the effects digital contact tracing and related tools have on vulnerable communities and make recommendations to correct any injustices attributable to the program as well as to enhance access.[160]

That same board also should assess proposed incentives or disincentives to encourage adoption of new technologies to ensure that they are equitable, non-coercive and do not discriminate directly or indirectly against any individual or group.[161] Access to public services and accommodations should not require use of any technology that does not meet these criteria and that has not been shown to improve public health outcomes.

Finally, the law should prohibit private companies from controlling the capabilities of digital contact tracing and other technologies used for public health surveillance or dictating their terms of use. As the Johns

---

158 Nagy, *supra* note 141 ("Authorities need to have a transparent plan for not only monitoring the effectiveness of these interventions in breaking transmission chains but also to guarantee against unintended consequences, particularly for already vulnerable or disenfranchised populations.").

159 The agenda outlined by a group of Swiss researchers is a useful starting point for assessing effectiveness. *See* von Wyl Viktor et al., *A Research Agenda for Digital Proximity Tracing Apps*, 2020 SWISS MED. WEEKLY 150 (2020), https://smw.ch/article/doi/smw.2020.20324.

160 *See* KAHN ET AL., *supra* note 59, at 7–8.

161 *See id*. at 8.

Hopkins Project on Ethics and Governance of Digital Contact Tracing Technologies has emphasized, the design of these technologies "should be capable of evolving depending upon local conditions, new evidence, and changing preferences and priorities."[162] This means that public health authorities, not technology companies, should control what they do and how they work.[163]

VI. CONCLUSION

"*An average of 3,100 people in the United States died of the coronavirus each day in January—one every 28 seconds.*"[164]

"*[T]he time lag between knowing when a case emerges inside,* **or even proximate to** *the home, and when an intercept team can be mobilized can literally save lives.*"[165]

"*[C]ontact tracing apps do not require tracking the location of individual users*."[166]

As I complete this Essay, we just endured the worst month of the pandemic. As the Washington Post article quoted above starkly states, in the U.S., deaths peaked in January 2021 at one every twenty-eight seconds. COVID-19 alone reduced overall life expectancy of Americans in 2020 by more than one year—the largest single-year decline in the past forty years.[167] That drop is far worse for communities hit hardest by this disease: falling by over two years for Black Americans and over three years for Latin Americans.[168]

As the second quote highlights, epidemiologists tell us that access to real-time information about who is contracting this deadly disease and where they live, even if it is not granular enough to identify exposure definitively, still can save lives. Would a better digital contact tracing app that included the option for users to collect and share that information with health authorities have made a difference? We do not know because we never tried. And we certainly did not know for sure that they would not back in May 2020 when the EDPB and many others

---

162 *Id.* at 2.

163 *Id.* at 2.

164 Karin Brulliard, *Three Days in the Deadliest Month in the Covid Pandemic*, WASH. POST. (Feb. 18, 2021), https://www.washingtonpost.com/health/interactive/2021/covid-death-toll-january

165 Curtis et al., *supra* note 121 (emphasis added).

166 *See* EDPB, *supra* note 59.

167 *See* Rob Stein, *Pandemic Shortens U.S. Life Expectancy, Study Concludes*, NPR (Jan. 15, 2021), https://www.npr.org/sections/coronavirus-live-updates/2021/01/15/957209935/pandemic-shortens-u-s-life-expectancy-study-concludes.

168 *Id.*

decided the answer must be no, even and while many apps were still proposing to try.[169]

It is just plain dumb that we never gave them a chance.

[169] *See* KHAN ET AL., *supra* note 59, at 2 (urging "an approach that recognizes that there are complicated issues to resolve for governments, institutions, and businesses and that introduction of [digital contact tracing technologies] must include public engagement and ongoing assessments to improve both performance and adoption.").