Saint Louis University Law Journal

Volume 65
Number 4 *Tradeoffs: Technology, Privacy, and the Law (Summer 2021)*

Article 6

2021

Balancing Public Health and Privacy: Lessons from Digital Contact Tracing for COVID-19 Vaccination Tracking Efforts

Carmel Shachar
The Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School, cshachar@law.harvard.edu

Follow this and additional works at: https://scholarship.law.slu.edu/lj

 Part of the Law Commons

Recommended Citation

Carmel Shachar, *Balancing Public Health and Privacy: Lessons from Digital Contact Tracing for COVID-19 Vaccination Tracking Efforts*, 65 St. Louis U. L.J. (2021).
Available at: https://scholarship.law.slu.edu/lj/vol65/iss4/6

This Childress Lecture is brought to you for free and open access by Scholarship Commons. It has been accepted for inclusion in Saint Louis University Law Journal by an authorized editor of Scholarship Commons. For more information, please contact Susie Lee.

BALANCING PUBLIC HEALTH AND PRIVACY: LESSONS FROM DIGITAL CONTACT TRACING FOR COVID-19 VACCINATION TRACKING EFFORTS

CARMEL SHACHAR*

ABSTRACT

The COVID-19 pandemic has brough the tension between individual privacy and public health initiative to the fore, in part because many of the solutions to the challenges of the pandemic proposed are digital. The first year of the pandemic has revealed that the Health Insurance Portability and Accountability Act is both too restrictive of traditional public health activities but also underprotective of important categories of health data. The failure of digital contact tracing applications to make a difference in combatting the pandemic during its early stages also illustrates the tension between individual privacy and public health surveillance. In order to harness the power of digital health to combat COVID-19 and other public health crises, we must resolve this tension through building trust in digital public health and modernizing our health data privacy regulation.

* Carmel Shachar, J.D., M.P.H., Executive Director, Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School.

There is an inherent tension between individual privacy and public health initiatives. Public health initiatives often benefit from access to detailed, comprehensive information on individuals, especially when it comes to combating infectious disease pandemics. On the other hand, individuals may have serious and valid objections to their data being used by these initiatives and concerns as to whether the data will be repurposed for other less noble causes after the objectives of the initiative have been achieved. The COVID-19 pandemic has brought that tension to the fore, especially since many of the solutions proposed are digital ones that rely on large amounts of information.

This paper will first explore the longstanding tension between individual privacy and public health interests found in the Health Insurance Portability and Accountability Act ("HIPAA"). It will then consider how the tension between privacy and public health undermined the use of digital contact tracing applications to address the COVID-19 pandemic. It will then consider the implementation of COVID-19 vaccine verification trackers as the next conflict between privacy and public health likely to flare. Lastly, the paper will suggest lessons to be learned from the unsuccessful implementation of digital contact tracing apps that could contribute to a better outcome for COVID-19 vaccine verification trackers.

I. CHALLENGES AND LIMITATIONS OF HIPAA

In the United States, medical data is largely governed by HIPAA, although some state statues such as the California Privacy Act ("CCPA") also can apply. Unfortunately, even pre-pandemic, HIPAA was considered outdated and increasingly ineffective at protecting data privacy within a modern, digital society.[1] The critiques of HIPAA most relevant to an infectious disease pandemic can perhaps be categorized into two buckets: 1) HIPAA is onerous to comply with, creating a chilling effect on public health research and surveillance; and 2) HIPAA is significantly limited in scope, focusing almost exclusively on electronic health records and ignoring the larger universe of health data.

HIPAA does include an exception for public health,[2] allowing covered entities to disclose protected health information ("PHI") to public health authorities legally authorized to receive such information, even without consent. Specifically, a covered entity:

> [M]ay disclose PHI to a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling

1. I. Glenn Cohen & Michelle M. Mello, *HIPAA and Protecting Health Information in the 21st Century*, 320 JAMA 231, 232 (2018).

2. *Bulletin: HIPAA Privacy and Novel Coronavirus*, U.S. DEP'T HEALTH & HUMAN SERV. (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf [https://perma.cc/E5VH-QT9Z].

> disease, injury, or disability, including, but not limited to, reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.[3]

There are of course, limitations to this exception. Most notably, the disclosure must be given to a *public health authority*, defined as a federal, state, tribal, or local agency responsible for the public's health under an official mandate.[4] This excludes health systems, nonprofits, and other non-governmental entities seeking to address public health concerns. Likewise, this definition suggests that other governmental agencies that are not officially mandated to be responsible for the public's health would not be able to receive this information under this exception.

Furthermore, this exception is permissive, not mandatory: covered entities are permitted to make such disclosures to public health authorities but are not required to do so.[5] Health care providers may be reluctant to disclose useful data to public health authorities since much of this PHI reveals sensitive information regarding health status or lifestyle, such as insights into sexual orientation, drug use and needle sharing, or mental health status.

As a result, it is unsurprising that HIPAA is perceived as a barrier to public health activities and research.[6] In a 2007 survey of epidemiologists, 67.8% of respondents reported that HIPAA had significantly made research more difficult, including adding costs and time to study completion.[7] This is hardly shocking because if public health experts cannot get access to data via the HIPAA public health exception—perhaps because they are not partnered with governmental authorities or because local providers are reluctant to share data and cannot be compelled to do so—then they must go the onerous route of obtaining informed consent for their activities. Even more concerning perhaps is that these respondents also felt that HIPAA had a greater negative influence on human subjects' protection than a positive impact, with only one quarter of respondents reporting that HIPAA enhanced privacy/confidentiality for public health research subjects.[8] This suggests that we are perhaps not gaining significant protections while imposing some challenging requirements for conducting public health research. While public health research is distinct from

3. 45 C.F.R. § 164.512(b)(i) (2016).

4. 45 C.F.R. § 164.501 (2013).

5. 45 C.F.R. § 164.512 (2016).

6. Andrea Wilson, *Missing the Mark: The Public Health Exception to the HIPAA Privacy Rule and Its Impact on Surveillance Activity*, 9 HOUS. J. HEALTH L. & POL'Y 131, 155 (2009).

7. Roberta B. Ness, *Influence of the HIPAA Privacy Rule on Health Research*, 298 JAMA 2164, 2164 (2007).

8. *Id.* at 2166.

public health activities, it is likely that HIPAA has a similar impact on those initiatives as well.

If HIPAA is too restrictive on traditional public health activities, it is also significantly under-protective of important categories of health data at the same time. HIPAA was written at a time before the digital revolution, in a world pre-smart phones and apps.

Correspondingly, its authors focused almost exclusively on PHI found within electronic health records ("EHRs"). Health data that is not handled by health care providers or entered into an EHR is considered "outside of HIPAA."[9] Unfortunately, this means that some very personal information is left largely unregulated and unprotected. For example, a research team was able to create an algorithm that uses Instagram social media posts to diagnose depression as a higher success rate than (human) general practitioners.[10] Target famously used data analytics to identify which consumers are pregnant based on their past shopping history, sometimes even before the individuals themselves knew of their pregnancies.[11] Because of HIPAA's focus on traditional medical providers, its blind spots often benefit non-traditional participants in health and wellness, such as technology companies. The limits of HIPAA may be problematic because they can cause individuals to feel cynical regarding data privacy. If Target or Amazon is already using my data to flag if I am pregnant or sick, then do I have any real privacy protections? The more data is used in ways that serve companies and not individuals, the more individuals may worry that any information put out there will be fair game for usages they do not support or agree with. Furthermore, the uneven distribution of privacy regulations can become pertinent during an infectious disease pandemic because of the heightened incentives for new players to develop health related solutions to control or mitigate outbreaks. When companies, not longstanding hospital systems or public health institutions, lead the development of pandemic digital solutions, does that erode trust in these solutions for consumers?

II. LEARNING FROM THE CONTACT TRACING EXPERIENCE

Digital contact tracing, sometimes also called exposure notification, is a logical response to the challenges of the COVID-19 pandemic. Manual contact tracing can quickly be overwhelmed by the large number of individuals to process in an infectious disease pandemic that spreads quickly through a given population. Although many states, such as Maryland, Massachusetts, and New

9. Cohen & Mello, *supra* note 1, at 231.

10. Andrew G. Reece & Christopher M. Danforth, *Instagram Photos Reveal Predictive Markers of Depression*, 6 EPJ DATA SCI. 1, 1 (2017).

11. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html [https://perma.cc/546W-CQC9].

York, rapidly scaled up their manual tracing programs,[12] this increase in capacity is likely still not sufficient to meet demand.[13] Digital contact tracing, however, can easily scale with a rapidly growing pandemic. Another benefit that digital contact tracing has over manual contact tracing is that notifications can happen almost instantaneously from when the index case is reported, i.e., the digital contact tracing system almost immediately notifies those who may have been exposed.[14] By delivering notice to those possibly exposed and infected faster, the digital contact tracing system can potentially reduce infections by encouraging those individuals to quarantine earlier. Lastly, manual contact tracing relies on individuals knowing the names and information of those they came into contact with during their period of infectiousness. This can lead to overlooking proximity to strangers, such as riding in an elevator or waiting in line for coffee together. Digital contact tracing does not have this limitation because it relies on proximity of phones and smart devices rather than human knowledge. Of course, the optimal system may combine digital contact tracing with follow up manual contact tracing to gain a better sense of the scenarios that result in disease spread or to connect those infected to social and medical services.[15] But it is clear that digital contact tracing can be a powerful tool in combating COVID-19 and other infectious diseases.

Despite its promises, digital contact tracing has remained relatively underutilized in the United States and other countries.[16] Digital contact tracing apps are only really effective when a significant percentage of the population has downloaded and used them. Iceland has the highest adoption rate of any country that does not mandate digital contact tracing apps, with forty percent of the population using them.[17] In Europe, the adoption rates ranged from around twenty percent in Germany to seven percent in Italy to three percent in France.[18] These low rates of adoption translate into very few instances of possible transmission being caught. For example, in France, with its minimal adoption

12. Katherine Faulders et al., *States Race to Start Coronavirus Contact Tracing, a Monumental Task Ahead*, ABC NEWS (Apr. 22, 2020, 3:02 PM), https://abcnews.go.com/US/states-race-start-coronavirus-contact-tracing-monumental-task/story?id=70285156 [https://perma.cc/EUJ2-ZEX3]; Christie Aschwanden, *Contact Tracing, a Key Way to Slow COVID-19, Is Badly Underused by the U.S.*, SCI. AM. (July 21, 2020), https://www.scientificamerican.com/article/contact-tracing-a-key-way-to-slow-covid-19-is-badly-underused-by-the-u-s/ [https://perma.cc/2L3L-3QSR].

13. Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, 368 SCIENCE 1, 2 (2020).

14. *Id.* at 1.

15. Louise C. Ivers & Daniel J. Weitzner, *Can Digital Contact Tracing Make Up for Lost Time?*, 5 LANCET PUB. HEALTH e417, e418 (2020).

16. Mitch Leslie, *COVID-19 Fight Enlists Digital Technology: Contact Tracing Apps*, 6 ENGINEERING (BEIJING) 1064, 1066 (2020).

17. *Id.* at 1065.

18. *Id.*

rate, the national contact tracing app caught only fourteen cases of possible transmission.[19] The low rates of adoption can be exacerbated in the United States, where there is no national leadership on this issue and funding for a federal tracing and testing program was cut from COVID-19 relief bills.[20] Instead, states and municipalities are creating their own digital contact tracing apps, which may or may not communicate with each other. In areas that cross state borders, such as the tri-state area including New York City but also the New Jersey and Connecticut suburbs, this can result in a patchwork of different apps that are unable to adequately flag potential transmission events. This is dismaying because best estimates suggest that to be truly effective, eighty percent of smartphone users or fifty-six percent of the general population of a country must download and use a digital contact tracing app.[21]

III. WHY DID DIGITAL CONTACT TRACING FAIL?

We must ask ourselves: knowing the value of digital contact tracing to combat a deadly pandemic with no yet known treatments, why did this technology have such little impact? A significant factor is likely the tension between individual privacy and public health surveillance. This tension was expressed in two ways: 1) by designing apps to maximize privacy, potentially at the cost of effectiveness; and 2) by the reluctance of consumers to adopt these apps, even when maximized for privacy.

Digital contact tracing apps have been designed on a privacy preserving spectrum. On one hand, some countries such as China explicitly link individual identities to their COVID-19 risk, limiting movement of certain people based on whether they may be at risk for the disease, and Israel and South Korea have chosen to use cell phone geolocation data to digital contact trace their populations without any of sort of opt-out.[22] Most countries, however, have balked at such Orwellian oversight and attempted to enshrine privacy protections directly into the architecture of their apps. Norway discontinued use of its digital contact tracing app after it was critiqued by the Norwegian Data Protection Authority.[23] Many have based their apps on a joint Apple/Google platform that utilizes Bluetooth technology to avoid identifying individuals or tracking their locations but still is able to identify when two people have spent

19. *Id.*

20. Aschwanden, *supra* note 12.

21. Patrick H. O'Neill, *No, Coronavirus Apps Don't Need 60% Adoption to be Effective*, MIT TECH. REV. (June 5, 2020), https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/ [https://perma.cc/H6CM-WTGL].

22. Michelle M. Mello & C. Jason Wang, *Ethics and Governance for Digital Disease Surveillance*, 368 SCIENCE 951, 952 (2020).

23. Reuters Staff, *Norway to Halt COVID-19 Track and Trace App on Data Protection Concerns*, REUTERS (June 15, 2020, 5:25 AM), https://www.reuters.com/article/us-health-coronavirus-norway-apps-idUSKBN23M18T [https://perma.cc/6DQC-T365].

enough time in proximity to transmit the virus. In fact, both Ireland and Germany switched from building their own digital contact tracing app to using the Apple/Google technology because of the strong privacy protections offered by the Apple/Google approach.[24] Most American states are also using this platform.

It is possible, however, that some effectiveness is lost by adopting such privacy focused architecture. As mentioned above, Bluetooth based digital contact tracing tracks proximity and not geolocation. However, for tracking and controlling an infectious disease pandemic, location is actually more useful. For example, if a person reports positive for COVID-19, public health authorities will want to be able identify everyone who was near them, not just those with Bluetooth enabled contact tracing on their phones. Knowing that the person spent time at the local supermarket would allow authorities to post signs at that store notifying those who regularly shop there to get tested. The emphasis on privacy also means that not all crucial information will be shared with critical partners. One European protocol, DT-3P, only allows for health authorities to be notified if the COVID-19 positive individual chooses to allow it.[25] While not all countries have adopted this protocol, it is aligned with the Apple/Google approach.[26]

Obviously, this greatly undermines the ability of public health authorities to adequately respond to the pandemic and utilize all data available. Furthermore, many digital contact tracing apps rely on individuals to self-report or to give permission for their health care provider to report their COVID-19 test results. It is unknown how many individuals may test positive but decline to enter this information into the system, perhaps due to fears of oppression in the form of a mandatory quarantine order triggered by reporting this data. This means that the digital contact tracing system will not be able to be utilized for some percentage of cases, even though those individuals may have the app installed. This is problematic because success breeds success. When there were few stories about COVID-19 digital contact tracing apps resulting in lowered transmission rates, individuals had little incentive to download these apps or to continue to use them.

Similarly, another impediment to widespread adoption of digital contact tracing was likely consumers' fears about the usage of their data and lack of trust in the institutions developing the applications. A study in Australia demonstrated that higher levels of trust in data privacy was strongly predictive of the probability of downloading the digital contact tracing app available to those

24. Charlotte Jee, *Is a Successful Contact Tracing App Possible? These Countries Think So*, MIT TECH. REV. (Aug. 10, 2020), https://www.technologyreview.com/2020/08/10/1006174/covid-contract-tracing-app-germany-ireland-success/ [https://perma.cc/C6R3-A3R9].

25. I. Glenn Cohen et al., *Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension*, 323 JAMA 2371, 2371 (2020).

26. *Id.* at 2372.

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

individuals.[27] Conversely, lower levels of trust in data privacy are a likely reason for reluctance to use a digital contact tracing app. In most countries in which digital contact tracing apps were not made mandatory, the significant levels of awareness of privacy and personal data concerns—i.e., the lack of trust—meant that it was a significant challenge to get individuals to actually use these apps.[28]

Individuals are wise to be wary and have low levels of trust in data privacy, at least in some jurisdictions. In the United States there was little to prevent technology companies from using this valuable data for further purposes, including commercialization, although there were some attempts to legislate this issue.[29] In the United States, digital contact tracing apps were unlikely to be governed by HIPAA unless they involved a covered entity as discussed above.[30] Therefore, it was unclear to individuals how their data would be used beyond the initial purpose of COVID-19 contact tracing. This could be a significant contribution to a lack of trust in data privacy. For example, there were fears during the Black Lives Matter protests that digital contact tracing was going to be used to identify and punish protestors.[31] By contrast, European users of digital contact tracing apps are better protected by the General Data Protection Regulation ("GDPR") which governs not only medical data but virtually all data generated.[32] Despite these additional protections, the limited adoption of digital contact tracing apps in Europe, fairly comparable to the rates of adoption in the United States, demonstrates that European users are perhaps similarly skeptical of these applications.

IV. COVID-19 VACCINATION: THE NEXT INTERSECTION OF PUBLIC HEALTH AND PRIVACY

The next collision between public health and privacy will be in the form of COVID-19 vaccine tracking. As of this writing, the Food and Drug Administration has granted emergency use authorization for COVID-19 vaccines created by Pfizer/BioNTech, Moderna, and Johnson & Johnson.[33]

27. Nicholas Biddle et al., *Data Trust and Data Privacy in the COVID- 19 Period*, AUSTL. NAT'L U. 1, 24 (2020), https://csrm.cass.anu.edu.au/sites/default/files/docs/2020/7/Data_trust_and_data_privacy_in_the_COVID-19_period.pdf [https://perma.cc/7GBX-RXCS].

28. Robert A. Fahey & Airo Hino, *COVID-19, Digital Privacy, and the Social Limits on Data-Focused Public Health Responses*, 55 INT'L J. INFO. MGMT. 1, 1 (2020).

29. Carmel Shachar, *Protecting Privacy in Digital Contact Tracing For COVID-19: Avoiding A Regulatory Patchwork*, HEALTH AFFAIRS BLOG (May 19, 2020), https://www.healthaffairs.org/do/10.1377/hblog20200515.190582/full/ [https://perma.cc/FU6Y-85GK].

30. *Id.*

31. Fahey & Hino, *supra* note 28, at 4.

32. Shachar, *supra* note 29.

33. Colin Dwyer, *Moderna's COVID-19 Vaccine Becomes 2nd to Earn FDA Authorization*, NPR (Dec. 18, 2020, 7:45 PM), https://www.npr.org/sections/coronavirus-live-updates/2020/12/18/947948227/modernas-covid-19-vaccine-becomes-2nd-to-earn-fda-authorization [https://perma.cc/LXD6-T475].

There are several other pharmaceutical companies working to create and obtain approval for their own COVID-19 vaccines in the US and other jurisdictions, including a collaborative effort by Oxford University and AstraZeneca[34] and another developed by Novavax.[35] If 2020 was the year of a global pandemic, 2021 will be the year of mass vaccinations across the globe.

Public health, as expressed both through government initiatives and the actions of private actors, requires not only individuals to be vaccinated for COVID-19 but also to be able to track who has been vaccinated and who has not been. Because COVID-19 is highly infectious, some countries, such as Hungary and Iceland, may require proof of immunity—either through antibodies or vaccination—before allowing non-citizens to enter.[36] As vaccination becomes more commonplace, more and more countries will likely require proof of COVID-19 immunity for travel. States may require COVID-19 vaccination for those working with vulnerable populations, such as staff in a nursing facility, or for university students. Municipalities that rely on public transportation may require some sort of COVID-19 proof of vaccination before individuals are permitted to use their buses and trains. Employers may go beyond those limited mandates, to require COVID-19 vaccination of their employees returning to the workplace. Restaurants, concert venues, and sports games may also require proof of vaccination so that they can avoid inadvertently playing host to a super-spreader event or even advertise their venues as COVID free.[37]

In some ways, requiring COVID-19 vaccination and disclosure of vaccination status will not be new. Traditionally, states and municipalities have required proof of vaccinations, or documentation of why exemptions should be granted, for children attending school.[38] States have also required certain employers, especially hospitals, to require vaccinations and to track proof of vaccinations for their employees. Famously, in *Jacobson v. Massachusetts*, the Supreme Court acknowledged that states have very broad powers to implement immunization requirements to protect public health.[39] On the other hand, COVID-19 vaccination requirements will probably be more far reaching than

34. Maria Deloria Knoll & Chizoba Wonodi, *Oxford–AstraZeneca COVID-19 Vaccine Efficacy*, 397 THE LANCET 72, 72 (2020).

35. Paul T. Heath et al., *Safety and Efficacy of NVX-CoV2373 Covid-19 Vaccine*, NEW ENG. J. MED. (June 30, 2021), https://www.nejm.org/doi/pdf/10.1056/NEJMoa2107659?listPDF=true [https://perma.cc/NPR3-FM97].

36. Scott McLean & Florence Davey-Attee, '*Immunity Passports' are Already Here. But They Come with Warnings*, CNN TRAVEL (Dec. 7, 2020), https://www.cnn.com/travel/article/hungary-iceland-covid-immunity-passport-scn/index.html [https://perma.cc/XAV6-JL3R].

37. Jane C. Hu, *Now That COVID-19 Vaccines Are Here, So Is the Prospect of Digital Immunity Passports*, SLATE (Dec. 18, 2020, 12:23 PM), https://slate.com/technology/2020/12/what-are-covid-19-digital-immunity-passports.html [https://perma.cc/EC3K-3YTJ].

38. Carmel Shachar & Dorit Reiss, *When Are Vaccine Mandates Appropriate?*, 22 AMA J. OF ETHICS 36, 37 (2020).

39. 197 U.S. 11, 11–12 (1905).

SAINT LOUIS UNIVERSITY SCHOOL OF LAW

most vaccine requirements because of the impact that COVID-19 has had on society. Many vaccine requirements are limited to children attending school, which would allow adults to continue to live and work in these communities even if they did not agree with the vaccine mandate. The unprecedented reach of the COVID-19 vaccination efforts will likely give rise to litigation and policy debates.

2021 will also be a year of conflict between individuals' interest in keeping their vaccination histories private and public health efforts to track vaccination efforts. A significant percentage of Americans have indicated that they do not want to receive the COVID-19 vaccine, according to polling conducted both by the Kaiser Family Foundation and the Pew Research Center.[40] The number of vaccine skeptics and those reluctant increases in communities of color, which may be the result of a complicated history with the medical establishment.[41] Individuals may resent having to disclose their vaccination status in order to use public transportation, shop in person, go to their offices, and live their daily lives. They may also worry how this data will be used for purposes beyond immediate access.

Furthermore, the architecture of vaccine tracking is unclear: currently the Centers for Disease Control ("CDC") provides COVID-19 vaccination cards that are meant to be a reminder to patients to get their second dose and not proof of vaccination.[42] Health care providers can provide vaccination records, just as they do with other vaccines, but this may be complicated by the fact that many individuals will be receiving their COVID-19 vaccines through their workplaces, local pharmacies, or other alternative providers. Technology companies and industry sponsors are working to fill this void, with airlines laying the groundwork to use CommonPass, currently an app used to show that users have tested negative, for vaccine verification purposes.[43] The parallels to digital contact tracing are striking: industry leadership resulting in a potentially fragmented market and with questionable data privacy protections.

40. Liz Hamel et al., *Race, Health, and COVID-19: The Views and Experiences of Black Americans*, KFF 1, 4 (Oct. 13, 2020), http://files.kff.org/attachment/Report-Race-Health-and-COVID-19-The-Views-and-Experiences-of-Black-Americans.pdf [https://perma.cc/2JPC-D56Z]; Cary Funk & Alec Tyson, *Intent to Get a COVID-19 Vaccine Rises to 60% as Confidence in Research and Development Process Increases*, PEW RES. CTR. 1, 4 (Dec. 3, 2020), https://www.pewresearch.org/science/wp-content/uploads/sites/16/2020/12/PS_2020.12.03_covid19-vaccine-intent_REPORT.pdf [https://perma.cc/VL84-FFTT].

41. Hamel et al., *supra* note 40.

42. Akshay Syal, *Covid Vaccine Cards are a Reminder for the Second Shot, Not a Passport*, NBC NEWS (Dec. 4, 2020, 8:49 AM), https://www.nbcnews.com/health/health-news/covid-vaccine-cards-are-reminder-2nd-shot-not-passport-n1249941 [https://perma.cc/8ECH-6FMW].

43. Hu, *supra* note 37.

V. LESSONS TO LEARN FOR COVID-19 VACCINE TRACKING

It is vitally important that we learn from the failure of digital contact tracing when implementing COVID-19 vaccine verification tracking. Otherwise, we run the risk of botching the implementation of a valuable tool in combating the COVID-19 pandemic. Additionally, we should use this opportunity to consider the historical shortcomings of the American data privacy regulation scheme when it comes to novel uses of technology in public health.

Foremost, we should consider the importance that trust plays in the adoption of digital solutions to public health concerns. The digital contact tracing efforts incorporated privacy-preserving efforts into the digital architecture, in the form of Bluetooth technology. This was a good step, allowing developers to tout that their apps could not gather certain sensitive information, such as geolocation data. Nevertheless, this choice in and of itself was probably not sufficient to resolve the tension between public health and individual privacy interests. The fragmentation of the digital contact tracing market and the leadership from companies that are unregulated by HIPAA, such as technology companies, likely did not inspire confidence from users. Simply telling consumers that technology companies have pledged to respect privacy is not enough. It is extremely important that institutions that require the use of COVID-19 vaccine verification trackers, be they government entities such as transportation authorities or private companies such as concert halls, be transparent in way that this data may or may not be used. As these verification trackers are developed there should be an opportunity for community representatives to provide feedback so that these apps reflect the local privacy expectations and norms.

Another take away may be that success helps foster confidence and adoption. Digital contact tracing apps based on Bluetooth had some serious limitations, such as requiring the individual to voluntarily enter COVID-19 test results. Because of these limitations, the apps were always going to be of somewhat limited use to prevent the spread of COVID-19. Without any success stories of note, there was little to inspire individuals to download these apps and use them. There are parallels to the response to vaccination requirements: in scenarios where authorities over relied on mandates there was significant pushback, including riots at times.[44] Vaccine campaigns were more successful when mandates were accompanied by educational efforts, to help individuals understand why participating in this public health initiative was beneficial to them. If there had been more education and outreach regarding digital contact tracing apps, then perhaps adoption rates would have increased. This would have resulted in more chains of transmission being broken, creating a feedback loop of success. Governments should consider educational campaigns to help

44. Shachar & Reiss, *supra* note 38, at 40.

individuals understand why verifying COVID-19 vaccination status before entering public spaces is so important.

Lastly, because of the importance of tracking both COVID-19 infections and vaccinations, the United States should consider data privacy legislation targeted at digital solutions to these public health problems. HIPAA is too limited to reach digital contact tracing apps and vaccine verifications trackers because it focuses on traditional medical providers. Passing targeted legislation focused on building trust among individual users of these digital solutions would help significantly with adoption of vaccine verification trackers. Individuals could be assured that their data would really only be used for certain uses. This may even allow us to structure these digital solutions to maximize their effectiveness rather than to maximize privacy protections.

The tension between public health initiatives and privacy interests is a longstanding one, as demonstrated by the challenges that HIPAA has in both being over and under-protective of privacy when it comes to public health activities. Nevertheless, digital contact tracing has shown us that the tension between public health and privacy can significantly undermine important digital solutions that can address infectious disease pandemics. There is now a significant chance that the same tension will undermine our ability to track COVID-19 vaccination efforts. In order to avoid the same mistakes as digital contact tracing, we should be careful to foster trust, through education, through incorporation of community norms, and through targeted legislation.