Contact Tracing and Privacy amid the COVID-19 Pandemic

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Sean Burtner

April 6, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Sean Burtner

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

Contact Tracing and Privacy amid the COVID-19 Pandemic

The COVID-19 pandemic has presented countless challenges for public health systems. High infectivity combined with asymptomatic cases has complicated transmission control, demanding rigorous contact tracing protocols. Public health authorities have looked to meet this demand by employing smartphone contact tracing apps to partly automate the process; while they view this technology as essential disease intervention, other groups hesitate to adopt the technology, with some critics even warning that digital contact tracing could "turn into dystopian surveillance devices" (Collins, 2020). Such stark opposition warrants an investigation into how public health authorities, privacy advocates, and other social groups in the U.S. have competed to draw the line between essential contact tracing and undue invasion of privacy.

According to Ferretti et al. (2020), where traditional contact tracing has typically been laborious and slow, contact tracing apps could introduce efficiencies capable of "[achieving] epidemic control if used by enough people." One study found that with an 80% adoption rate among smartphone users, digital contact tracing could effectively suppress the epidemic (Hinch et al., 2020). Therefore, for contact tracing to be successful, it must be trusted. Understanding the reservations of privacy advocacies such as the American Civil Liberties Union (ACLU) and Electronic Frontier Foundation (EFF), as well as the confidence of public health agencies such as the U.S. Centers for Disease Control and Prevention (CDC), is the first step in promoting such trust. However, privacy advocacies and public health agencies alike have recognized the critical role of trust in contact tracing technology, which has prompted a battle for this trust. In other words, these groups have primarily competed to establish contact tracing's role in the pandemic by vying for public trust or distrust in both the technology and institutions responsible for implementing it.

Review of Research

Researchers have examined common misgivings about contact tracing techniques, and have proposed theoretical methods for addressing them. According to McClain and Rainie (2020), a major concern among users is the government's ability to keep personal data safe; they found that approximately 40% of potential users are not confident that public health departments will adequately protect sensitive data. Ferretti et al. (2020) found that in order for the technology to be perceived as ethical, the institutions deploying it must make numerous compromises, some of which could address this lack of confidence. These compromises include establishing an oversight committee containing members of the public, agreeing on a set of guiding ethical principles, and enforcing careful protections on data use, among others. With such provisions, Ferretti et al. argue, the public is significantly less likely to perceive the technology as a dangerous invasion of privacy that jeopardizes personal data. Ahmed et al. (2020) similarly found that organizers of contact tracing technology can mitigate user concern by exhibiting "complete transparency" and instituting "legislative guarantees against misuse of data." However, these studies fail to cite how public health authorities have implemented these compromises in practice, or how privacy advocates have applied their resources to demand them.

Furthermore, according to Altmann et al. (2020), transparent, yet stringent, security measures are necessary in order to counteract distrust in government and "concerns about cybersecurity and privacy." They identify these reservations as a primary impediment to adoption of the technology. Keusch et al. (2019) draw analogous conclusions in their study on general user perception of mobile data collection. They also found other common barriers to adoption include lack of incentive and insufficient information about the technology. Again, these studies contain insufficient discussion about the ways in which the agencies responsible for

the technology have attempted to address public concern. Blasimme and Vayena (2020) contend that a "piecemeal creation of public trust" is required to validate digital contact tracing in the public eye. Achieving this trust, according to Blasimme and Vayena, requires strategies such as adaptive governance and design, proof of effectiveness, and legislative oversight. The researchers refer to examples of such strategies being employed in countries such as Switzerland and France, but do not account for instances in the United States.

Research on the give-and-take between public health authorities and privacy advocates has largely been limited to foreign countries. Leslie (2020) examines how governments worldwide have approached ethical deployment of contact tracing technology, finding that countries have trended toward decentralized apps that "do not share personal information" in order to meet privacy concerns. The research alludes to similar initiatives in the U.S., though remains at an overly general scope. Abeler et al. (2020) further analyze data protections in different contact tracing app designs. They primarily cite technology developed by the Singaporean government which incorporates "privacy by design" to preserve anonymity. Lapolla and Lee (2020) similarly study the tradeoffs of "privacy versus safety in contact-tracing apps" and how various actors have advocated for protections. Their study focuses on European interventions, most notably a Belgian petition opposing centralized contact tracing systems. In summary, current studies do not sufficiently analyze the strategies employed by social groups in the U.S. to establish the role and image of contact tracing technology.

However, the clash between privacy rights and technology is not a novel issue. Extensive research has been conducted on similar dynamics, particularly with regard to online targeted advertising. This technology relies on the passive data collection of user activity in order to work, similar to digital contact tracing. Toubiana et al. (2010) suggest that while "[targeted

advertising] is inherently in conflict with privacy," precautions such as increased transparency, opt-out options, and rigorous data protections were crucial compromises in promoting acceptance of targeted advertising. Goldfarb and Tucker (2011) also contend that governments have adopted privacy regulations in targeted advertising to respond to consumer concern, but conclude that excessively stringent restrictions reduce efficacy. Evans (2009) examined how developers of the technology, such as Google, answered criticism by "consumer privacy advocates and regulators" regarding the capture and storage of Internet browsing data; Evans suggests that familiarizing the public with the technology and considering public opinion in its design contributed to its acceptance. Implementations of these ideas in the analogous context of digital contact tracing has yet to be satisfactorily investigated.

Advocating for Privacy Protections

Contact tracing advocates actively promote security and privacy best practices to increase public trust. Although the CDC is not responsible for implementing contact tracing, they issued publicly available guidelines describing the "minimum and preferred features of digital contact tracing tools" for health departments to better address "personal privacy and data security" (CDC, 2020a). Not only does this serve state and local health departments in implementing effective contact tracing, but it also demonstrates an awareness for prudent security and privacy measures, furthering the CDC's goal to "build trust and confidence" in contact tracing (Moore et al., 2020). Public health experts at the Johns Hopkins Center for Health Security outlined the need for "extensive [privacy] safeguards" and "responsible data management" in contact tracing technology to "reassure concerned citizens and privacy activist groups that sensitive information will be respected" (Watson et al., 2020). In the Virginia Department of Health's (VDH) contact tracing guidebook, the VDH promotes principles pertaining to privacy and confidentiality as an

avenue for “building and sustaining trust/cooperation from community members” (VDH et al., 2020). Another government agency, the Federal Trade Commission (FTC), published guidance on how to distinguish a “contact tracing text message scam” from a “legitimate text message” sent by a health department (Tressler, 2020). The FTC offers reassurance that personal privacy and sensitive data are protected in the contact tracing system. These institutions recognize the role of trust in implementing effective contact tracing, and advocate for privacy safeguards to gain such trust.

Beyond simply advocating for safeguards, privacy activists strongly call for the legal establishment of privacy protections in contact tracing. In April 2020, the Electronic Privacy Information Center (EPIC) urged Congress to regulate digital contact tracing, claiming that it is essential to “implement standards that safeguard privacy” (Rotenberg et al., 2020); EPIC proceeded to delineate numerous requirements related to privacy for Congress to enforce. Public Knowledge, a digital policy advocacy, expresses similar sentiments by stressing “the responsibility of policymakers to create rules and systems that protect privacy” with regard to digital contact tracing (Collins, 2020). Furthermore, the EFF contends that “a comprehensive data privacy law is long overdue,” citing the shortcomings of existing U.S. laws (Schwartz, 2020). In California, the EFF publicly “called on Governor Newsom to place basic privacy guardrails on any contact-tracing program run by or with the state” (Tsukayama, 2020). Another advocacy, the ACLU, claims that contact tracing systems “should adopt the strongest possible…legal safeguards” in regard to data and privacy (Gillmor, 2020). By urging the government to establish legal protections, these advocacies inevitably cast doubt on the security and privacy of a contact tracing system sans such protections; this pushes the perception of contact tracing toward that of a gratuitous privacy violation rather than a trustworthy tool.

A Question of Necessity

Public health authorities and developers of contact tracing technology seek to garner trust by rationalizing the need for contact tracing during a pandemic. In a press release from Apple, a developer of digital contact tracing, they state that their technology will "help governments and health agencies reduce the spread of the virus" and "accelerate the return of everyday life" (Apple, 2020). Similarly, the CDC identifies contact tracing as "a key strategy for preventing further spread of COVID-19," explaining that a successful implementation of the process provides valuable insight (CDC, 2020b). Among the advantages, according to the World Health Organization (WHO), is the ability to "identify risk factors" and develop "targeted public health and social measures" (WHO, 2021). In encouraging adoption of statewide contact tracing technology, the VDH argues that it will "reduce your risk while protecting your family, friends and community" (VDH, 2020); public health experts at Johns Hopkins make similar claims that a robust system of contact tracing is necessary "in order to save lives" and "make progress toward returning to work and school" (Watson et al., 2020). According to these experts, digital contact tracing is an important component of a comprehensive health system, calling it a "force-multiplying" technology that facilitates strategic resource use. By vindicating contact tracing as an element of the pandemic response, these groups demonstrate that they act in the best interest of the public, who in turn, are more likely to offer their trust.

Conversely, privacy advocates have challenged the efficacy of contact tracing. According to the ACLU, contact tracing systems "potentially [risk] people's privacy without bringing them benefits" (Gillmor, 2020). They argue that without strong testing and treatment services, "[contact tracing] does nothing to help stem the spread of COVID." The EFF also maintains that "no [contact tracing] app will work absent widespread testing" (EFF, 2020). A major concern is

the risk of diverting resources away from other public health measures that may reap more benefit. A consumer advocacy called Public Citizen has minimal faith in workplace contact tracing apps in particular, arguing that "none of them have been proven to be effective at mitigating the spread of COVID-19" (Public Citizen, 2020). Without a proof of efficacy, they refuse to trust the technology. Public Knowledge warns of the potential for a low adoption rate of digital contact tracing such that the overall efficacy of the system is severely limited. The risk that contact tracing apps are ineffective deters users, "thereby limiting the [apps'] effectiveness" itself (Collins, 2020). This self-fulfilling prophecy hinders uptake and subsequent success of the technology; users doubt its efficacy, limiting adoption rate, which in turn reduces the efficacy and confirms the users' misgivings. Public Knowledge recognizes this cycle as a major downfall of digital contact tracing. Highlighting the potentially limited efficacy of contact tracing calls its necessity into question, further diminishing public trust in the system.

Growing Skepticism

Privacy advocates also raise suspicion regarding the intentions of the institutions deploying contact tracing to promote distrust. The EFF cautions against "companies that harvest and monetize our personal information" as they "will not look beyond their own balance sheets to consider the privacy harms" of their technology (Tsukayama, 2020). These "short-sighted" companies are merely making "land grabs for our data" and "[trading] our information away," the EFF claims. Additionally, the ACLU considers the pandemic "an opportunity for would-be authoritarians and powerful corporations to expand their power" (Gillmor, 2020). They insinuate that those responsible for implementing contact tracing are ill-intentioned, deliberately designing the systems to be "decidedly privacy-unfriendly." Media Alliance, another digital privacy advocacy, states that there are "reasonable fears" that "law enforcement agencies might use

access to contact tracing data to harass low-income communities" (Rosenberg, 2021). They point to incidents involving law enforcement and people of color as a reflection of morally flawed intentions in these agencies. EPIC similarly fuels doubt by calling on Congress to "investigate" the "companies and government agencies involved in digital contact tracing" to verify their intentions with regard to user privacy (Rotenberg et al., 2020). In expressing such concerns, these advocacies generate skepticism about the integrity of the contact tracing system and its overseers, strengthening its perception as an invasion of privacy.

Privacy advocates further promote distrust in contact tracing systems by drawing attention to the danger of data misuse. In a letter to former Vice President Mike Pence, EPIC and numerous other civil rights groups note an "explosion of privacy violations" and "manipulative data practices" in data aggregation technology due to the lack of adequate privacy legislation (EPIC et al., 2020). Without such legislation, these groups warn, contact tracing technology can directly undermine privacy and equity. According to Public Citizen, contact tracing systems in the workplace inherently misuse data; they claim that "workplace coronavirus tracings apps institute dystopian mass surveillance by default" (Public Citizen, 2020). Public Citizen further argues that some contact tracing apps fail to handle data securely, citing violations of the Health Insurance Portability and Accountability Act (HIPAA). Public Knowledge likewise contends that contact tracing technology comes with the unacceptable cost of making "highly sensitive location data available for exploitation" (Public Knowledge, n.d.). Media Alliance recognizes historical "violations of data-sharing limitations of all kinds" within law enforcement agencies, and warns of similar violations in the implementation of contact tracing (Rosenberg, 2021). They emphasize that in a poorly implemented system, personal data could be publicly accessible on the Internet or dark web, where stolen data is often leaked. These hazards relating to the use of

personal data in contact tracing generate fear and skepticism about the reliability of these systems. Privacy advocates take advantage of this by highlighting such hazards, thereby increasing public distrust in the technology.

Transparency and Information Influence Trust

Privacy advocacies generate additional doubt by explicitly calling for transparency from the institutions responsible for implementing contact tracing technology. Public Knowledge called on lawmakers to take initiative in this endeavor and "create an environment of transparency and accountability" (Collins, 2020). According to Collins, "it won't matter what privacy protections" are in place if transparency is not a fundamental component of the system. In their letter to Pence, EPIC et al. (2020) requested that leaders in contact tracing efforts are "transparent about the collection and use of personal and aggregate information," and that they accomplish this by "opening the process" to "experts from public health, data security, [and] privacy." They necessitate a collaborative effort rather than an exclusive task force on the grounds of public trust. EPIC, in their statement to Congress, reinforced this call for transparency by arguing that the "governments, companies, or entities deploying these systems [should] prove that they are necessary, effective, lawful, and protect privacy" (Rotenberg et al., 2020). The EFF similarly claims that the institution deploying contact tracing technology has a responsibility to "demonstrate that it is effective and respects [user] privacy" by "sharing privacy policies" and "explaining how and by whom" data is used (Gebhart et al., 2020). These efforts to achieve transparent communication serve to caution the public against an unchecked contact tracing system and consequently fuels their distrust.

Public health authorities have conversely looked to build trust by familiarizing and informing the public with regard to the contact tracing process. In the VDH's guidebook on

contact tracing, they recommend "avoiding terms like 'agent' or 'official'" when referring to those affiliated with contact tracing to make the process "seem less intimidating" and "build comfortability" (VDH et al., 2020). Furthermore, the VDH released a contact tracing app called COVIDWISE for the state of Virginia, and in the app's description, they explicitly describe "How COVIDWISE Works" and "How COVIDWISE Protects Your Privacy" (VDH, 2021). Keeping users informed is clearly a priority for the VDH in gathering support and trust for their technology. The CDC adopts a similar approach, stating that "to help generate understanding and acceptance of contact tracing… [CDC develops] new and engaging resources about contact tracing for the general public" (Moore et al., 2020). They further acknowledge that informing the public is part of their effort to both "promote trust in the public health department" and "dispel misconceptions" about contact tracing. The WHO represents another public health organization that recognizes the power of information in building trust; they published a set of ethical considerations to guide digital contact tracing, within which "transparency and explainability" are emphasized (WHO, 2020). Providing individuals with "concise and reader-friendly information…regarding the purpose of [data] collection" and other features of the technology is an important tool for increasing public acceptance, according to the WHO. Public health authorities from all of the discussed groups have employed similar informative tactics to foster familiarity in the technology, and thereby promote trust.

Conclusion

As Blasimme and Vayena (2020) state, contact tracing technology suffers from a "typical social control dilemma." Demonstrating its effectiveness, and therefore necessity, is extremely difficult without first achieving widespread adoption. However, promoting adoption is likewise

difficult to accomplish without a proof of efficacy. This circular dilemma is only solvable with substantial public trust, both in the technology and those managing it.

However, such trust is a precious commodity in the realm of mobile data aggregation. Public perception of this technology is scarred by invasions of privacy, lack of transparency, and incidents of data misuse; privacy advocates have highlighted these threats to invoke caution and distrust. In order to successfully implement digital contact tracing in the United States, public health authorities and developers of the technology must overcome these doubts. Involving the public in the development and oversight process, establishing strong privacy safeguards, and clearly communicating such safeguards will be important tactics in this endeavor.

These strategies can be generalized for other data aggregation technologies where users hesitate to offer their trust. Similar technologies are likely to invite similar skepticism, which can be accounted for in advance based on this research. Further research can be conducted on the competition of social groups in other countries with regard to digital contact tracing and privacy. Additionally, as the world begins to leave the COVID-19 pandemic behind, hindsight investigation can be conducted into the specific successes and failures of digital contact tracing deployment in the United States. Gaining more insight into how to overcome the deep-rooted skepticism that deters initial uptake is imperative, as this dictates the technology's efficacy and thus its ability to alleviate public health burdens – now, and in the future.

References

Abeler, J., Bäcker, M., Buermeyer, U., & Zillessen, H. (2020). COVID-19 contact tracing and data protection can go together. *JMIR mHealth and uHealth*, *8*(4), e19359. https://doi.org/10.2196/19359

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Seneviratne, A., Hu, W., Janicke, H., & Jha, S. K. (2020). A survey of COVID-19 contact tracing apps. *IEEE Access*, *8*, 134577-134601. http://doi.org/10.1109/access.2020.3010226

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., & Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth*, *8*(8), e19857. https://doi.org/10.2196/19857

Apple. (2020, April 10). Apple and Google partner on COVID-19 contact tracing technology. Apple Newsroom. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

Blasimme, A., & Vayena, E. (2020, November 13). What's next for COVID-19 apps? Governance and oversight. *Science*, *370*(6518), 760–762. https://doi.org/10.1126/science.abd9006

CDC (2020a). U.S. Centers for Disease Control and Prevention. Guidelines for the implementation and use of digital tools to augment traditional contact tracing. Centers for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf

CDC (2020b, December 3). U.S. Centers for Disease Control and Prevention. Case investigation and contact tracing: part of a multipronged approach to fight the COVID-19 pandemic. Centers for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html

Collins, S. (2020, April 17). Privacy-protective contact tracing depends on more than an API. Public Knowledge. https://www.publicknowledge.org/blog/privacy-protective-contact-tracing-depends-on-more-than-an-api/

EFF (2020). Electronic Frontier Foundation. COVID-19 and digital rights. Electronic Frontier Foundation. https://www.eff.org/issues/covid-19

Electronic Privacy Information Center, Campaign for a Commercial Free Childhood, Center for Democracy & Technology, Center for Digital Democracy, Constitutional Alliance, Consumer Action, Consumer Federation of America, Media Alliance, MediaJustice, Oakland Privacy, Parent Coalition for Student Privacy, Privacy Rights Clearinghouse, Public Citizen, Public Knowledge, & Rights x Tech. (2020, May 5). EPIC, coalition to

White House: Set privacy standards for COVID-19 data and technology uses. Electronic Privacy Information Center. https://epic.org/2020/05/epic-and-14-other-groups-tells.html

Evans, D. (2009). The online advertising industry: Economics, evolution, and privacy. *The Journal of Economic Perspectives*, *23*(3), 37-60. https://www.jstor.org/stable/27740539

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491). http://doi.org/10.1126/science.abb6936

Gebhart, G., Hoffman-Andrews, J., & Crocker, A. (2020, July 30). University app mandates are the wrong call. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/07/university-app-mandates-are-wrong-call

Gillmor, D. K. (2020, April 16). Principles for technology-assisted contact-tracing. American Civil Liberties Union. https://www.aclu.org/report/aclu-white-paper-principles-technology-assisted-contact-tracing

Goldfarb, A., & Tucker, C. (2011). Privacy regulation and online advertising. *Management Science*, *57*(1), 57-71. https://www.jstor.org/stable/41060701

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., Lythgoe, K., Cruz, A. B., Zhao, L., Stewart, A., Ferretti, L., Parker, M., Meroueh, A., Mathias, B., Stevenson, S., Montero, D., Warren, J., Mather, N. K., Finkelstein, A., Abeler-Dörner, L., Bonsall, D., & Fraser, C. (2020, April 16). Effective configurations of a digital contact tracing app: A report to NHSX. University of Oxford. https://045.medsci.ox.ac.uk/files/files/report-effective-app-configurations.pdf

Keusch, F., Struminskaya, B., Antoun, C., Couper, M. P., & Kreuter, F. (2019). Willingness to participate in passive mobile data collection. *Public Opinion Quarterly*, *83*(1), 210-235. https://doi.org/10.1093/poq/nfz007

Lapolla, P., & Lee, R. (2020). Privacy versus safety in contact-tracing apps for coronavirus disease 2019. *Digital health*, *6*, 2055207620941673. https://doi.org/10.1177/2055207620941673

Leslie M. (2020). COVID-19 Fight Enlists Digital Technology: Contact Tracing Apps. *Engineering (Beijing, China)*, *6*(10), 1064–1066. https://doi.org/10.1016/j.eng.2020.09.001

McClain, C., & Rainie, L. (2020, October 30). The challenges of contact tracing as U.S. battles COVID-19. Pew Research Center. https://www.pewresearch.org/internet/2020/10/30/the-challenges-of-contact-tracing-as-u-s-battles-covid-19/

Moore, M., Scofield, J., Sendak, M., Kreger, M., Gray, M., Herrera, A., & Valladares, A. (2020, December 9). Building the bridge: Community trust and contact tracing during COVID-19 [Video]. CDC Webinars. https://emergency.cdc.gov/epic/learn/2020/webinar_20201209.asp

Public Citizen. (2020, August 13). Report: Workplace coronavirus tracing apps institute dystopian mass surveillance by default. Public Citizen. https://www.citizen.org/news/report-workplace-coronavirus-tracing-apps-institute-dystopian-mass-surveillance-by-default/

Public Knowledge. (n.d.). Communications policy solutions for the pandemic. Public Knowledge. https://www.publicknowledge.org/communications-policy-solutions-for-the-pandemic/

Rosenberg, T. (2021, January 8). Will COVID-19 contact tracing expand state surveillance? Media Alliance. https://media-alliance.org/2021/01/will-covid-19-contact-tracing-expand-state-surveillance/

Rotenberg, M., Fitzgerald, C., & Butler, A. (2020, April 15). EPIC to Congress: Establish privacy safeguards for digital contact tracing. Electronic Privacy Information Center. https://epic.org/2020/04/epic-to-congress-establish-pri.html

Schwartz, A. (2020, May 28). Two federal COVID-19 privacy bills: A good start and a misstep. EFF. https://www.eff.org/deeplinks/2020/05/two-federal-covid-19-privacy-bills-good-start-and-misstep

Toubiana, V., Narayanan, A., Boneh, D., Nissenbaum, H. F., & Barocas, S. (2010). Adnostic: Privacy preserving targeted advertising. Proceedings Network and Distributed System Symposium. https://ssrn.com/abstract=2567076

Tressler, C. (2020, May 19). COVID-19 contact tracing text message scams. Federal Trade Commission. https://www.consumer.ftc.gov/blog/2020/05/covid-19-contact-tracing-text-message-scams

Tsukayama, H. (2020, September 9). California still needs privacy protections for COVID tracking apps. EFF. https://www.eff.org/deeplinks/2020/09/california-still-needs-privacy-protections-covid-tracking-apps

Virginia Department of Health. (2020). COVIDWISE. Virginia Department of Health. https://www.vdh.virginia.gov/covidwise/

Virginia Department of Health, COVID-19 Unified Command Health Equity Working Group, Access and Functional Needs Advisory Committee for the Virginia Department of Emergency Management, Commonwealth of Virginia Equity Leadership Task Force, & Virginia Department of Emergency Management. (2020, July). COVID-19 testing and contact tracing health equity guidebook. Virginia Department of Health.

https://www.vdh.virginia.gov/content/uploads/sites/76/2020/07/Testing-and-Contact-Tracing-Health-Equity-Guidebook-July-2020.pdf

Virginia Department of Health. (2021). COVIDWISE app store preview. Apple. https://apps.apple.com/us/app/covidwise/id1518059690

Watson, C., Cicero, A., Blumenstock, J., Fraser, M., Hosandadi, D., Inglesby, T., Martin, E., Meyer, D., Montague, M., Mullen, L., Nuzzo, J., Potter, C., Rivers, C., Sell, T. K., Shearer, M., Trotochaud, M., Warmbrod, K. L., Watson, M., George, D., Gurley, E., Lane, J. T., Marx, M., Plescia, M., & Sharfstein, J. (2020, April 10). A national plan to enable comprehensive COVID-19 case finding and contact tracing in the US. Center for Health Security. https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf

WHO. (2020, May 28). World Health Organization. Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. World Health Organization. https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

WHO. (2021, February 1). World Health Organization. Contact tracing in the context of COVID-19. World Health Organization. https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19