Trust Deficit: Why a Lack of Trust in Government and Technology has Harmed U.S. Pandemic Response

Position Statement for Privacy & Pandemics: Responsible Uses of Technology and Health Data During Times of Crisis

By Sara Collins, Policy Counsel at Public Knowledge and Erin Simpson, Associate Director of Technology Policy at the Center for American Progress
September 30th, 2020

Word Count: 995, footnotes excluded.

Following the police murder of George Floyd in Minneapolis, Minnesota, protesters nationwide took to the streets to protect Black lives and demand police accountability in the United States. Occurring in the midst of the coronavirus crisis, a Minnesota public safety commissioner reached for an ill-advised metaphor in discussing the investigation of protestors at a weekend press conference: similar to COVID-19 he said, we're "contact tracing"[1] the protesters: "Who are [the protesters] associated with? What are they advocating for?...We are in the process right now of building that network."[2]

Minnesota public health authorities were quick to clarify that the police were in fact *not* "contact tracing" the protestors[3], but the damage was done: his words inadvertently legitimized fears that data from public health contact tracing would be used for policing purposes.

In facing the coronavirus crisis, a lack of public trust in both government and technology has complicated public health response in the United States. As we prepare for future public

---

[1] Contact tracing is a longstanding public health process used in infectious disease response. It seeks to identify infected persons, inform them of possible exposure, and ask them to take appropriate steps to stop further spread. Commonly, public health officials receive information about individuals who test positive for a disease of interest and then conduct interviews with those people about their relationships and places they've visited in order to contact those people and prevent further spread. For more, see: Watson, Crystal et al. "A National Plan to Enable Comprehensive COVID-19 Case Finding and Contact Tracing in the US," *Johns Hopkins Center for Health Security*, April 10 2020, https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf.

[2] The moment was emblematic of the uphill battle that contact tracers were already facing in overcoming fears arising from historical and contemporary abuses of power during public health crises and a tide of misinformation online. Police misconduct during the protests further complicated their work by further damaging that trust, especially within the Black community. See: Ng, Algred. "Contact tracers concerned police tracking protestors will hurt COVID-19 aid," *Cnet*, June 01 2020, https://www.cnet.com/news/contact-tracers-concerned-police-tracking-protesters-will-hurt-covid-19-aid/; Hallerman, Tamar. "False info online complicates contact tracing efforts," *The Atlanta-Journal Constitution* via *Government Technology*, May 22 2020, https://www.govtech.com/security/False-Info-Online-Complicates-Contact-Tracing-Efforts-.html; Stobbe, Mike. "Mass Gatherings, Erosion of Trust Upend Coronavirus Control," *US News & World Report*, June 01 2020, https://www.usnews.com/news/health-news/articles/2020-06-01/mass-gatherings-erosion-of-trust-upend-coronavirus-control.

[3] Ibid.

health and environmental crises, a government that is not worthy of trust will continue to impede public response. The scope of repairing such trust is vast. One part of that effort must include developing meaningful privacy safeguards, which will increasingly be a prerequisite to effective public response.

At the outset of the coronavirus crisis, public health experts recognized that capacity constraints in public health systems made them unable to match the speed or scope of COVID-19's spread: even extremely well-resourced, modern public health systems are limited in their ability to contact trace at the scale and speed as a novel coronavirus outbreak.[4] In an effort to close that gap, public health experts and technologists rushed to develop various systems to aid public health response, with Apple and Google's partnership to incorporate exposure notification features[5] into their smartphones emerging as a dominant system. While critical equity[6], governance, and implementation issues remain, exposure notification systems have the potential to fill that gap by providing speed and scope that can complement the slower, higher fidelity, more strategic work of contact tracing[7].

As has been widely emphasized, such an exposure notification system is a complement, not a substitute, for traditional public health contact tracing.[8] As has been less emphasized, an

---

[4] Feretti, Luca et al. "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, May 08 2020, https://science.sciencemag.org/content/368/6491/eabb6936.full. ; Hellewell, Joel et al. "Feasibility of controlling COVID-19 outbreaks by isolation of case and contacts," *The Lancet: Global Health*, February 28 2020, https://www.thelancet.com/journals/langlo/article/PIIS2214-109X(20)30074-7/fulltext#seccestitle10.

[5] For a discussion of the initial Google Apple offering in the context of ongoing open source approaches, including the Temporary Contact Number Coalition members and the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) project, see "Fundamental technology questions" here: Simpson, Erin & Conner, Adam. "Digital Contact Tracing to Contain the Coronavirus," *Center for American Progress*, April 22 2020, https://www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-tracing-contain-coronavirus/. ; More on the Google Apple system here: *Exposure Notifications: Using technology to help public health authorities fight COVID-19*, https://www.google.com/covid19/exposurenotifications/. ; For resources on use of the Google Apple standard through open source applications, see the Linux Public Health Foundation resources here: *Collaborating to Battle COVID-19*, Linux Foundation Public Health, 2020, ://www.lfph.io/.

[6] Landau, Sausan, Lopez, Christy E. & Moy, Laura. "The Importance of Equity in Contact Tracing," *Lawfare*, May 01 2020, https://www.lawfareblog.com/importance-equity-contact-tracing. ; Bagchi, Koustubh et al. "Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns," *New America Open Technology Institute*, July 02 2020, https://newamericadotorg.s3.amazonaws.com/documents/Safra-OTI-NA_Contact_Tracing_Paper.pdf.

[7] Simpson, Erin & Conner, Adam. "Digital Contact Tracing to Contain the Coronavirus," *Center for American Progress*, April 22 2020, https://www.americanprogress.org/issues/technology-policy/news/2020/04/22/483521/digital-contact-tracing-contain-coronavirus/.

[8] Allen, Daniel et al. "Roadmap to Pandemic Resilience: Massive Scale Testing, and Supported Isolation as the Path to Pandemic Resilience for a Free Society." *Edmond J. Safra Center for Ethics*, April 20 2020, https://ethics.harvard.edu/files/center-for-ethics/files/roadmaptopandemicresilience_updated_4.20.20_1.pdf. ; Bagchi, Koustubh et al. "Digital Tools for COVID-19 Contact Tracing: Identifying and Mitigating the Equity, Privacy, and Civil Liberties Concerns," *New America Open Technology Institute*, July 02 2020,

exposure notification system is a privacy protective complement, especially in contrast to the practices of traditional contact tracing: officials receive PII and medical data and combine it with location data and details on social relationships in a variety of systems, including standard commercial software like Salesforce[9], with limited public oversight of the process. While extensive research on the efficacy of exposure notification systems is needed, initial results are promising.[10] If such results bear out, exposure notification systems could, on top of the existing public health response, fill the COVID-19 response gap regarding speed and scope and put more autonomy in people's hands. Complementing existing public health responses, this addition would be a more scalable and more privacy protective layer that is explicitly attuned to the risks of government surveillance and scope creep.

But adding to other sources of legitimate public mistrust in government, exposure notification systems must also overcome legitimate public distrust of technology. Some distrust has been driven by high profile data breaches and lax privacy laws.[11] But such feelings are primarily driven by the feeling that regular people no longer have any understanding of what data is collected, how it is being used, and that they have no way to take back control.[12]

These fears have perhaps been legitimated and exacerbated by the introduction of lesser privacy-protective exposure notification technologies. In the privacy-sensitive Apple/Google architecture, which is currently being used by nine U.S. states[13] and 30 countries,[14] there have been no reports of serious breaches or misuse, but the failures of lesser protective systems have damaged public opinion. A joint venture from North and South Dakota relied on centralized GPS tracking and shared users' locations data not only with health

https://newamericadotorg.s3.amazonaws.com/documents/Safra-OTI-NA_Contact_Tracing_Paper.pdf. ; others.

[9] *Governor Newsom Launches California Connected – California's Contact Tracing Program and Public Awareness Campaign*, Office of Governor Gavin Newsom, May 22 2020, https://www.gov.ca.gov/2020/05/22/governor-newsom-launches-california-connected-californias-contact-tracing-program-and-public-awareness-campaign/.

[10] Early research the efficacy in practice of apps built on the Google/Apple standard expected soon from Germany, Canada, and elsewhere. See: Aubeg, Matthew et al. "Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state," *medRxiv*, September 02 2020, https://www.medrxiv.org/content/10.1101/2020.08.29.20184135v1.

[11] Kanaan, Elie. "Tracing, Tracking, and Trust: Why Tech is on the Sidelines in Contact Tracing," *Street Fight*, August 07 2020, https://streetfightmag.com/2020/08/07/tracing-tracking-and-trust-why-tech-is-on-the-sidelines-in-contact-tracing/#.X3DBCi2ZOu4.

[12] Auxier, Brooke et al. "Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information," *Pew Research Center*, November 15 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[13] Hall, Zac. "Which U.S. states are using Apple's Exposure Notification API for COVID-19 Contact Tracing?" *9to5Mac*, September 22 2020, https://9to5mac.com/2020/09/22/covid-19-exposure-notification-api-states/.

[14] Rahman, Mishaal. "Here are the countries using Google and Apple's Covid-19 Contact Tracing API," *XDA Developers*, September 29 2020, https://www.xda-developers.com/google-apple-covid-19-contact-tracing-exposure-notifications-api-app-list-countries/.

authorities, but also with third-parties--a violation of its own privacy policy.[15] Los Angeles' choosing to partner with a company[16] that has a history of enabling surveillance and racism will likely deter the public, and marginalized populations in particular, from using the tool. The public is already primed to mistrust any public health surveillance applications, and these examples exacerbate and, in some cases, actualize those fears: that these apps will not protect their data and instead use it for commercial exploitation or government misuse and prosecution.

The largest hurdle to adoption of privacy-protective exposure notification technology is not technical nor governance challenges, but rather a poverty of public trust in government and technology. Public skepticism is necessary and warranted: crucially, it has helped prevent the adoption of privacy invasive tools during the crisis. But we must also grapple with the ways our collective distrust and lack of protections have hampered the COVID-19 response in the US and harmed the public interest, even in cases where risk is low. In Germany, the exposure notification team worked with the government's data protection and cybersecurity authorities from the start. These agencies became key validators, along with the open source and privacy communities. Even with the DPA onboard, team leaders cited communication and trust as their biggest challenges, saying that the project was "25% technical, 75% communication."[17] In the US, as we have even fewer assurances our rights will be followed and continual examples suggesting they would not, that communication challenge is even greater.

We need strong privacy protections that ensure our data is not used against us. By not having privacy leadership, we've made it significantly more difficult to encourage adoption of technology that actually benefits the public interest. Without a strong privacy baseline in place, data harms will continue, but we'll also keep missing opportunities to respond to public crises with appropriate technologies. Strong federal privacy protections--ending data abuse by corporations and government--are one part of earning and restoring public trust. Without it, our collective failures to respond to mass crises will continue.

The authors wish to acknowledge Adam Conner, Greg Guice, and Alyssa Martindale for their discerning feedback.

---

[15] Fowler, Geoffrey A. "One of the first contact-tracing apps violates its own privacy policy," *The Washington Post*, May 21 2020, https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/.

[16] Citizen, which previously released a peer-to-peer alerting app to combat neighborhood crime, despite the obvious risks of racial profiling. While the application doesn't proactively share information with local law enforcement, Dr. Nicol Turner Lee commented that it can "empower people to act as law enforcement, and we already know that's a problem," citing instances of discrimination and hyper-partisan interactions between users. See: Ashworth, Boone. "Inside Citizen, the App That Asks You to Report on the Crime Next Door," *Wired*, July 07 2020, https://www.wired.com/story/citizen/.

[17] Personal communication (Erin Simpson), with Head of the Department for "Digitization and Innovation" at the German Health Ministry, August 2020.