ACLU
CENTER FOR ADVOCACY & POLICY
California

Center for Advocacy & Policy
Telephone (916) 442-1036
Fax (916) 442-1743

May 27, 2020

Senator Holly Mitchell
Chair, Senate Budget Committee
State Capitol, Room 5080
Sacramento, CA 95814

Assemblymember Phil Ting
Chair, Assembly Budget Committee
State Capitol, Room 6026
Sacramento, CA 9581

Senator Richard Pan
Chair, Senate Budget Subcommittee 3
State Capitol, Room 5114
Sacramento, CA 95814

Assemblymember Joaquin Arambula
Chair, Assembly Budget Subcommittee 1
State Capitol, Room 6026
Sacramento, CA 95814

Re: Budget oversight for COVID-19 contract tracing

Dear Chairperson Mitchell, Chairperson Ting, Chairperson Pan and Chairperson Arambula:

Thank you for your commitment and efforts to protect public health during the COVID-19 pandemic. As the state responds to this crisis, we urge you to ensure that we do not build a surveillance infrastructure that will persist long after the pandemic is over. This letter articulates key principles that should guide any response to the pandemic that includes deployment of new technology or collection of people's personal information.

On May 8, 2020 the Department of Finance notified the legislature's fiscal committees of the state's plans to supplement two budget items with funds for two contact-tracing initiatives. These items include $8.7 million to develop a training program for new contact-tracing personnel and $18.7 million for development of a "data management platform" developed and operated by Accenture, Salesforce, and Amazon.[1] On May 22, the Governor announced the launch of a new state contact tracing program called California Connected.[2] To our knowledge, however, the Administration has not disclosed any details regarding the nature of the system being built, what information it would ingest and process, or the privacy and security protections implemented to protect the personal information stored in the system.

These details are important . As you know, any effort at large-scale contact tracing—whether undertaken by humans or aided by technology—has the potential to interfere with public health efforts, undermine trust, and violate individual rights if deployed incorrectly. In order to be effective, the need for privacy protections must be addressed at the outset. Without robust privacy assurances built into a transparent and accountable procurement and development process, people may refuse to participate—defeating the essential goal of protecting public health.

[1] May 8, 2020 Letter from California Department of Finance to Fiscal Committees, http://dof.ca.gov/budget/COVID-19/documents/5-8-20_Sec-36_JLBC_Notification_5-6_DPH_VV-CC.PDF (last visited May 26, 2020).
[2] *See* https://covid19.ca.gov/contact-tracing/

In this letter, we articulate principles that should inform any public health intervention that includes an additional technological component. We urge your committees to exercise their oversight duties to ensure that the details of the state's program are publicly evaluated so that these important measures deserve Californians' trust.

Core constitutional and privacy principles must guide any government's use of technology and personal information in response to the public-health crisis. The California Constitution guarantees an inalienable right to privacy for all Californians, articulated in the Privacy Amendment to Article I, Section 1, which protects the privacy rights of "all people." The Privacy Amendment was passed in response to the "modern threat to personal privacy" posed by increased surveillance and then-emerging data collection technology.[3] Voters added the Privacy Amendment specifically to prevent governments and businesses from "stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes."[4] These constitutional principles must guide any government response to the public-health crisis.

Public-health interventions must earn communities' trust in order to be effective. To deserve that trust, measures deploying technology to address the health crisis must be narrowly tailored to meet urgent needs, authorized only for the time period necessary to combat the virus, used exclusively for public-health purposes, and have strict evidence-based public-health benefits. And those government responses must build in transparency and oversight from the beginning, bringing communities into the crisis response rather than dictating that response.

For a team of human contact tracers supported by technological tools, it will be critical that they receive training with respect to how to protect the privacy of the people whose information they collect. As a first step, the collection, retention, use, and sharing of any information collected must comply with all applicable privacy laws. But more is necessary; the government must also take special care to guarantee people's privacy in a context in which people will be afraid for their health and also concerned about a government agency seeking potentially detailed information about their movements, associations, and activities. This is especially true for immigrants and other vulnerable communities. When the government agency is sharing information with large technology companies (as appears to be the case here) the importance of maintaining strong privacy protections takes on unique importance.

Similarly, any system that uses mobile phones to identify who may have been exposed to an infected person—*i.e.*, an "exposure notification" system—must take special precautions. These tools differ from human contact tracing as it has traditionally been done by health professionals, which typically relies on information collected through individual interviews to trace the chain of potentially infected people. On their own, app-based exposure notification systems cannot stem the spread of COVID-19 and are useful only if those who learn of possible exposures are able to get testing, counseling, and treatment, and to afford to take measures such as self-quarantine. These services must be widely and quickly available to everyone in order for app-based exposure notification to have the possibility of effectively supplementing trained human tracers.

---

[3] *White v. Davis*, 13 Cal.3d 757, 774 (1975).
[4] *Id.*

In assessing contact-tracing tools, whether serving as an aid for human tracers or notifying potentially exposed people through an app, the government should apply the following standards:

- **The intervention must be effective**. Governments should evaluate and set benchmarks for the efficacy of the technology, factoring in accuracy, risk of false positives/negatives, and known limitations. While contact tracing performed by humans is a well-established approach, hypothetical data management systems to support this human contact tracing must be assessed to ensure that they are effective.[5] Building and deploying a new back-end system in the midst of a crisis carries the very real risk of undermining, rather than aiding, existing contact-tracing infrastructure. In other contexts, we have already seen how failure to apply accuracy and effectiveness benchmarks may be adversely affecting public-health outcomes. For example, inaccuracies in antibody testing could give individuals a false sense of security or be improperly relied on to make public health decisions. Both human contact tracing using purpose-built tools and app-based exposure notification technology must be subject to similarly high efficacy standards, to ensure that information is not collected without guaranteeing a corresponding public-health benefit.

- **The interventions must be voluntary**. Governments should issue (and enforce) guidance to ensure that any participation in contact tracing (whether through human interviews or an app-based exposure notification system) cannot be a condition of housing, employment, attending school, using a public accommodation, health coverage, or any government service or benefit. Public health experts have found that coercive health interventions frequently backfire,[6] sparking counterproductive efforts to resist and undermine health measures. If people want to subvert a mandatory contact-tracing app, they can simply turn their phone off or leave it at home.

- **The interventions must be equitable**. The COVID-19 outbreak in the United States has disproportionately afflicted Black communities and other communities of color,[7] and people of color are given less (and often worse) health care, leading to worse health outcomes.[8] While it is not clear yet whether any exposure notification tool will be effective, any contact tracing program that fails to be delivered to the communities most in need, regardless of implementation challenges, and that does not specifically ensure that those communities are cared for, will exacerbate existing racial disparities in the effects of

---

[5] Josh Lederman, *Congress sounds alarm over inaccurate antibody tests*, NBC NEWS, https://www.nbcnews.com/politics/congress/congress-sounds-alarm-over-inaccurate-antibody-tests-n1194876 (last visited May 15, 2020).

[6] In early April, Utah deployed a system that was supposed to alert people entering the state that they should complete a survey with their name, address, phone number, email, and any potential symptoms or exposure to COVID-19. Three days later, the Utah Department of Emergency Management suspended the system after it became clear that it did not work; numerous individuals mistakenly received the alert though they were nowhere near one of the nine virtual checkpoints or were in fact leaving the state. ACLU of Utah, *Shiny Surveillance Tech Fails Again*, https://www.acluutah.org/blog/item/1613-shiny-surveillance-tech-fails-again (last visited May 15, 2020).

[7] Clyde W. Yancy, *COVID-19 and African Americans*, JAMA (2020), https://jamanetwork.com/journals/jama/fullarticle/2764789 (last visited May 15, 2020).

[8] Austin Frakt, *Race and Medicine: The Harm That Comes From Mistrust*, THE NEW YORK TIMES, January 13, 2020, https://www.nytimes.com/2020/01/13/upshot/race-and-medicine-the-harm-that-comes-from-mistrust.html (last visited May 15, 2020).

COVID-19. Contact tracing efforts must also take into account the fact that only 80% of people in the United States (and even fewer people who are elderly or disabled) have a smartphone.[9] We appreciate that the Administration has promised that every who tests positive will have access to COVID-19 related treatment, regardless of income, health insurance, or immigration status.[10] Presumably this treatment will meet rigorous standards and be fully and equally provided to all with due regard for the disproportionate harm suffered by communities of color. We applaud the Administration's inclusion of cultural competency in the newly launched training for human contact tracers; these individuals must have an understanding of the community in which they are operating in order to properly conduct interviews and ensure that any information collected is accurate and provided voluntarily.

- **Any information collected should be limited to what is necessary and should be deleted at the end of the crisis**. Information collected to address the present crisis should come with privacy limitations built in from the start. Any system—whether enabling human contact tracing or providing app-based exposure notification—should have technical, legal, and operational safeguards limiting how information can be accessed and used. Privacy protections must be built into the product by engineers to ensure that only people who need access to certain information can see it. Surveillance technologies in the U.S. have often been targeted at communities of color and immigrant communities. Accordingly, those communities—which are among the hardest-hit from the impact of COVID19—must be able to trust that any digital contact tracing tool will not be used to harm them and will only be used by public health officials. While the Administration has said that human contact tracers will not ask about immigration status, restrictions must be stronger. The contact tracers as well as the data management platform, forms, and other tools these contact tracers use must likewise not include any requests for information that could be related to or used to deduce immigration status. Furthermore, procurement and data-use contracts should clearly mandate robust privacy protections limiting the use of people's information solely for the purpose of detecting and treating the COVID-19 disease. While existing law provides important privacy protections, there should be no question whether the individuals and companies carrying out these functions are duty-bound to the highest standard of confidentiality. And the training programs for human contact tracers must provide clear instructions with respect to the limits on access and use of people's private information. Finally, the information collected from people should be deleted once the present crisis is over. A crisis should never be used to build a permanent infrastructure of surveillance.

- **Privacy protections must be enforceable.** Governments should commit to pursuing only efforts that include strong and enforceable privacy protections. Any information collected through a manual contact-tracing program should be accompanied by enforceable guarantees that the information will be maintained and used in accordance with those strong privacy protections. Information should be used to address only the current public-health crisis. Once the crisis is over, the information collected from people should be

[9] *Demographics of Mobile Device Ownership and Adoption in the United States*, PEW RESEARCH CENTER: INTERNET, SCIENCE & TECH, https://www.pewresearch.org/internet/fact-sheet/mobile/ (last visited May 15, 2020).
[10] https://covid19.ca.gov/contact-tracing/

deleted. And information should be maintained in a way that provides robust security and privacy protections. These principles apply both to technology developers, who should build protections into the technology, and to distributors of technology (like Apple and Google) who should refuse to distribute technology that is not accompanied by these protections. And when a government agency plans to store information collected for public-health reasons in a database operated by a private vendor, those vendors should offer the same robust protections, enforceable by people who can take the private vendors to court if their privacy is violated. While the Administration has said that human contact tracers will follow all privacy laws, including ensuring the confidentiality of information, restricting sharing, and limiting use to public-health purposes, such assurances are empty promises if no meaningful enforcement mechanism exists.

We urge you to ensure that any use of technology to address the present crisis reflects good technology and governance policies in accord with the principles identified above. We are happy to discuss these issues and any proposals under consideration.

Sincerely,

Kevin G. Baker
Director of Legislative Affairs

Becca Cramer-Mowder
Legislative Coordinator & Advocate

cc. Joe Stephenshaw, State Director, Senate Budget and Fiscal Review Committee
Christian Griffith, Chief Consultant, Assembly Budget Committee
Scott Ogus, Consultant, Senate Budget and Fiscal Review Committee
Andrea Margolis, Consultant, Assembly Budget Committee
Keeley Martin Bosler, Director, California Department of Finance
Dr. Bradley P. Gilbert, Director, California Department of Health Care Services
Hon. Hannah-Beth Jackson, Chair, Senate Judiciary Committee
Hon. Lena A. Gonzalez, Chair, Senate Committee on Pandemic Emergency Response
Hon. Mark Stone, Chair, Assembly Judiciary Committee
Hon. Ed Chau, Chair, Assembly Privacy and Consumer Protection Committee