Dear Governor Newsom, President Pro Tempore Atkins, Speaker Rendon, and honorable members of the California Assembly and Senate:

We are non-profit groups dedicated to defending privacy, and write today to urge you to place privacy at the heart of any contact-tracing program in California as the state looks to expand such programs.[1] Doing so will also help ensure greater success for these contact tracing programs as more Californians will feel safe participating in them knowing the information they provide to help fight the pandemic won't be used to deport them or build data-rich profiles for data brokers and advertisers.

Californians have a constitutional right to privacy, and it is vital that the state protect that right even in this time of unprecedented crisis. Crises often open the door to erroneous judgment, panicked decisions, and programs that—while well-intentioned—undermine people's constitutional right to privacy and prove difficult to roll back. It is imperative that governments protect their people's rights with enforceable guardrails to prevent unwarranted privacy invasions at a moment when people are at their most vulnerable. As a national leader in privacy and a leading voice in setting policy regarding the coronavirus, California must step up and do the right thing as it makes policy to address the effects of COVID-19.

Privacy does not stand in opposition to public health but instead is fundamental to the success of public health programs. As Kat Deburgh, Executive Director of the Health Officers Association of California, has acknowledged, "[m]aintaining public trust is important. People need to know that when they share information with public health officials, that information is kept safe and confidential, shared only when necessary and allowable by law." We can build that trust with assurances that such programs will guard the privacy of the information people provide to public health officials.

[1] Anderson, Cathie, and Darrell Smith. "Kaiser Permanente Donates $63 Million to Expand Tracing of Coronavirus Cases in California," August 12, 2020. https://www.sacbee.com/news/local/health-and-medicine/article244866162.html.

States that have placed invasive tracking into their apps, such as Utah, North Dakota, and South Dakota[2], have quickly run into serious problems with their contact tracing efforts. In Utah, the state ultimately stopped a GPS location tracking feature in its app to increase participation because its inclusion was not popular, as state epidemiologist Angela Dunn explained.[3]

To avoid the privacy failings—and the way those failings undermine public health responses to the pandemic—our organizations jointly request the following guardrails on contact tracing programs to respect basic privacy rights. These guardrails must apply to both manual contact tracing (for example, by interviewing patients) and to automated contact tracing (for example, by exposure notification apps). These guardrails are the very minimum that should be done to ensure the privacy of Californians; some of our organizations have and will continue to request additional guardrails.

A crucial privacy protection to ensure contact tracing is embraced by Californians is the rule of data minimization: collecting the least possible information necessary to accomplish contact tracing's public health goals. The information required for such programs can reveal much not only about a person's movements but also their religious and political associations, as well as unrelated medical or other personal conditions they may wish to keep private. A public health entity engaged in contact tracing, and any private entity contracting with a public health entity for this purpose, must be prohibited from collecting, retaining, using, or disclosing data except as necessary and proportionate to control the spread of COVID-19.

Such protections should apply to contact tracing programs regardless of who administers them. They are especially important when a private entity contracts with government to provide contact tracing services, given the inherent risk a private entity will try to monetize this sensitive data. To that end, we suggest ensuring all contracts, MOUs, and other agreements with private entities who in any way assist with contact tracing efforts contain language ensuring the private entity contracting with a public health entity for purpose of contact tracing: (i) shall not use data collected for that purpose for any other purpose, including but not limited to targeted advertising or any other commercial purpose; and (ii) shall not combine such data with any other data possessed by the private entity.

Contact-tracing programs should also be prohibited from discriminating against people on the basis of participation (or nonparticipation). No one should be kept out of a workplace, school, or restaurant because they declined to participate in a contact-tracing program. Additionally,

[2] Fowler, Geoffrey. "One of the First Contact-Tracing Apps Violates Its Own Privacy Policy," May 21, 2020. https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/.

[3] Wells, David. Utah to disable location tracking in 'Healthy Together' COVID-19 app. July 21, 2020. https://www.fox13now.com/news/coronavirus/local-coronavirus-news/utah-to-disable-location-tracking-in-healthy-together-covid-19-app/.

compulsory participation risks the quality of data; people may lie to a contact tracer about where they have been or who they have seen or leave their phone with a contract tracing app at home to avoid sharing information they feel risks their privacy or safety.

There must also be strong requirement to purge stale data. Tracing information can be valuable for the public health response to the pandemic in the short-term, but it is also very sensitive and can reveal a lot about a person, especially if it can be tied to a particular person or household or combined with other information to reidentify a particular person or household. Retaining data for a long period of time is also a security risk and makes such programs appealing targets for data thieves.

The best practice is to purge the data when it is no longer useful. A 30-day limit on the retention of all data collected by such programs would be appropriate. This should apply to all information, not only personal information that can be linked to a specific person or household. It is sometimes possible to re-identify even personal information that has been rigorously deidentified.[4]

We would not, however, object to a narrowly-crafted exception from this data purge rule for a limited amount of aggregated and de-identified demographic data (such as race and ethnicity) for the sole purpose of tracking inequities in public health response to the crisis, provided such retained data was aggregated at a high enough level (such as census tract) to prevent re-identification.[5]

Several of our groups support two bills currently in the legislature, A.B. 1782 and A.B. 660, which, as currently drafted, contain these important protections as well as others many of our groups support. We appreciate the work that the authors of these bills—Asms. Ed Chau, Buffy Wicks, and Marc Levine—have put into doing the right thing for all Californians. We will continue to work with them to get these important bills passed.

As the state continues to respond to the ongoing pandemic, partner with companies, and invest state funds in contact tracing programs to track the virus, we urge you to ensure all new pandemic responses include these crucial privacy protections from the beginning and existing efforts have these privacy protections added in immediately and retroactively. Doing so will help

[4] Lubarsky , Boris. “Re-Identification of ‘Anonymized’ Data.” Georgetown Law Technology Review, September 14, 2018. https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.; Electronic Frontier Foundation. “Amicus Brief from EFF.” Electronic Frontier Foundation, October 6, 2011. https://www.eff.org/document/amicus-brief-eff-0/.

[5] Crocker, Andrew and Jacob Hoffman-Andrews. “How to Protect Privacy When Aggregating Location Data to Fight COVID-19,” May 2, 2020. https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

establish much-needed trust in these programs, which will in turn increase their efficacy in addressing the current public health crisis. It is also simply the right thing to do.

We thank you for your time and consideration.

Sincerely,
ACLU of California
Electronic Frontier Foundation
Oakland Privacy
Media Alliance
Privacy Rights Clearinghouse
Consumer Reports