July 31, 2020

The Honorable Ed Chau
State Capitol
P.O. Box 942849
Sacramento, CA 95814

The Honorable Buffy Wicks
State Capitol
P.O. Box 942849
Sacramento, CA 95814

Re: AB 1782 on COVID-19 privacy – support if amended

Dear Asm. Chau and Asm. Wicks:

We are six organizations dedicated to protecting consumer privacy. We write to thank you for your leadership in sponsoring AB 1782, as amended on July 14. This legislation would help protect the privacy of people in California whose personal information is processed by technology-assisted contact tracing for purposes of containing the COVID-19 outbreak. We would be pleased to support AB 1782 if amended to more fully protect the people's privacy interests in COVID-related information, as set forth below.

1. California needs COVID-19 privacy legislation.

Many government agencies and corporations are collecting people's personal information to respond to the COVID-19 crisis. Some states are deploying automated contact tracing apps, sometimes known as exposure notification systems.[1] States also are conducting manual contact tracing, often with private contractors,[2] and partnering with businesses to create websites where people are asked to hand over health and other information to obtain screening for COVID-19 testing and treatment.[3] The federal government is sharing

[1] https://www.theverge.com/2020/5/20/21265052/apple-google-coronavirus-notification-system-states-alabama-north-dakota-south-carolina.

[2] https://www.cnbc.com/2020/05/08/new-york-city-partners-with-salesforce-on-coronavirus-contact-tracing-program-mayor-says.html.

[3] https://www.eff.org/deeplinks/2020/03/verilys-covid-19-screening-website-leaves-privacy-questions-unanswered; https://pamplinmedia.com/pt/9-news/463149-375819-critics-oregon-covid-19-symptom-checker-raises-privacy-concerns-pwoff.

COVID-19 tracking data with its own corporate contractors, including TeleTracking Technologies[4] and Palantir.[5]

There are many ways to misuse COVID-related data. Some restaurants, for example, are collecting contact information from patrons to notify them later of any infection risk;[6] disturbingly but not surprisingly,[7] in at least one reported case a restaurant employee used a patron's information to send them multiple harassing messages.[8] Companies might divert information collected to address the pandemic to advertising.[9] All this information about people is also at risk of being stolen by identify thieves, stalkers, and foreign nations.[10]

Unfortunately, existing privacy laws do not adequately protect people from misuse of COVID-related data. For example, federal HIPAA protections of health data apply only to narrowly defined healthcare providers and their business associates.[11] That's why California needs strong, comprehensive consumer privacy legislation.[12] Unfortunately, we don't yet have it.

Thus, to meet the ongoing public health crisis, we need COVID-specific privacy legislation.

2. AB 1782 would help protect privacy in the pandemic.

AB 1782, as amended on July 14, contains important privacy safeguards relating to automated COVID-19 contact tracing apps, which the bill calls "Technology-Assisted Contact Tracing" (TACT).

First, TACT operators must obtain an individual's ***opt-in consent*** before collecting, using, maintaining, or disclosing their data. *See* Sec. 1924.3(a); *see also* Secs. 104002(b), 22364(a), 22366(b). Consent must be an unambiguous affirmative act, and any request for consent must disclose the purpose of processing. *See* Sec. 1924(b); Sec. 1924.1(a). Even after consent is granted, TACT operators must provide a simple means for a user to

4 https://www.nytimes.com/aponline/2020/07/15/us/ap-us-virus-outbreak-health-data.html.

5 https://www.washingtonpost.com/technology/2020/07/01/warren-hhs-data-collection/.

6 https://www.vice.com/en_us/article/g5ppa7/washington-restaurants-will-collect-diners-personal-info-for-coronavirus-tracking.

7 https://abcnews.go.com/Politics/att-employees-bribed-1m-unlock-phones-install-malware/story?id=64802367; https://www.washingtonpost.com/news/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/.

8 https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12332073.

9 https://www.eff.org/deeplinks/2019/10/twitter-unintentionally-used-your-phone-number-targeted-advertising; https://www.eff.org/deeplinks/2019/03/facebook-doubles-down-misusing-your-phone-number.

10 https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

11 https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

12 https://www.eff.org/deeplinks/2019/06/effs-recommendations-consumer-data-privacy-laws; https://www.eff.org/deeplinks/2019/12/sen-cantwell-leads-new-consumer-data-privacy-bill.

revoke consent, *see* Sec. 1924.1(b), and to temporarily disable or remove TACT components, *see* Sec. 1924.1(f). These are important safeguards.

Second, all public and private entities are ***prohibited from discriminating*** against people on the basis of participation (or nonparticipation) in TACT. *See* Sec. 1924.4. No one should be kept out of a workplace, school, or restaurant because they declined to participate in a contact-tracing program.

Third, TACT operators must ***minimize*** their collection, use, maintenance, or disclosure of data. Specifically, they cannot process data unless doing so is reasonably necessary to provide a service that a user requested. *See* Sec. 1924.3(b). *See also* Secs. 104002(c)(1), 22366(a), 22366(c), & 22366(d). This duty to minimize data processing is independent of the duty to obtain consent, and provides an added layer of privacy protection.

Fourth, TACT operators ***cannot associate*** their TACT data with other data. *See* Secs. 1924.5(c), 104002(d), & 22366(e). Combining data sets generates more detailed individual profiles, and carries heightened privacy risks.

Fifth, TACT operators have a ***60-day deadline to delete*** personal information, after collection. *See* Sec. 1924.1(e). COVID-19 has a 14-day incubation period,[13] so older information will not aid in addressing the current crisis. But that information can still be stolen, misused, and harnessed for inappropriate purposes.

Sixth, a public entity that is not a public health entity cannot deploy TACT, *see* Sec. 104002(a), or enter into a TACT contract, *see* Sec. 22362(a). Given the privacy risks posed by this technology, it is important to limit which kinds of government entities may deploy it. For example, law enforcement officials must not deploy it.

Finally, TACT operators must: (a) provide users an effective means to access, correct, and delete their personal information, *see* Sec. 1924.1(d); (b) publish quarterly reports about their processing, *see* Secs. 1924.1(h) & 104004(b); and (c) secure the data they process, *see* Sec. 1924.1(i).

3. AB 1782 should be strengthened.

While AB 1782 is a good start, California should do more to protect our COVID-related data privacy.

First, we need ***effective enforcement*** of these privacy rights with a private right of action. We suggest the following: "Any person may bring a lawsuit against any public entity or business that violates any of these rules, and a successful plaintiff may have the remedies of injunctive and declaratory relief, actual damages, liquidated damages of $100 per

[13] https://www.cdc.gov/coronavirus/2019-ncov/hcp/clinical-guidance-management-patients.html.

violation, and reasonable attorney fees." Private causes of action are a standard feature of legislation that protects people from governmental and corporate wrongdoing.[14]

Second, we need a stronger requirement to ***purge stale data***. As discussed above, AB 1782 sets a 60-day purge deadline, which is good. But it only applies to "personal information," *see* Sec. 1924.1(e), meaning data that could reasonably be linked to a specific person or household, *see* Sec. 1924(d). Thus, businesses and public entities that collect TACT data would be free to retain it forever, so long as it cannot reasonably be associated with a person or household. Yet it is sometimes possible to re-identify even personal information that has been rigorously deidentified.[15] So the 60-day purge rule should extend to *all* TACT data, whether or not it could reasonably be linked to an individual. However, we would not 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) just for purposes 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.[16]

Third, we need a ***ban on location tracking*** as part of TACT. Location data (such as GPS and cell site location) is not sufficiently granular to identify whether two people were close enough together to transmit COVID-19. But it is sufficiently precise to show whether a person attended a protest, a worship service, or a hospital appointment. Thus, location tracking invades privacy without advancing public health.[17] It might be possible to use Bluetooth-based proximity data to provide automated exposure notification in a privacy-preserving manner.[18] But such systems must not use location data.

Fourth, we need strong privacy protections for ***manual contact tracing***. AB 1782 addresses only automated contact tracing, and specifically excludes "traditional" contact tracing through "interviews" and the like. *See* Sec. 104008. Another pending California bill, AB 660 (Levine), addresses all contact tracing, but only provides two safeguards: a ban on sharing contact tracing data, except with a public health entity; and a ban on law enforcement participation in contact tracing.[19] Many of the additional safeguards in AB 1782 for automated contact tracing should also apply to manual contact tracing, including consent, non-discrimination, and data minimization. As explained above, there are myriad ways that manual contact tracing can invade privacy.

[14] https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy.
[15] https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/; https://www.eff.org/document/amicus-brief-eff-0.
[16] https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.
[17] https://www.eff.org/deeplinks/2020/03/governments-havent-shown-location-surveillance-would-help-contain-covid-19.
[18] https://www.eff.org/deeplinks/2020/05/governments-shouldnt-use-centralized-proximity-tracking-technology; https://www.eff.org/deeplinks/2020/04/apple-and-googles-covid-19-exposure-notification-api-questions-and-answers; https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing.
[19] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB660.

* * *

Again, we thank you for your leadership in carrying AB 1782, which contains important safeguards for TACT and COVID-related personal information. We look forward to supporting AB 1782 if it is amended as discussed above.

Sincerely,

Adam Schwartz
Senior Staff Attorney
Electronic Frontier Foundation

Jake Snow
Technology and Civil Liberties Attorney
ACLU of Northern California

Ariel Fox Johnson
Senior Counsel, Policy and Privacy
Common Sense Media

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America

Maureen Mahoney
Policy Analyst
Consumer Reports

Meghan Land
Executive Director
Privacy Rights Clearinghouse

cc: Senate Judiciary Committee