August 14, 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 as amended 8/11/20

Dear Asm. Chau and Asm. Wicks:

We are six organizations dedicated to protecting consumer privacy. We write to thank you for your leadership in authoring AB 1782, as amended on August 11. We support this bill in its current form. 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.

1. California needs COVID-19 privacy legislation.

Many government agencies and corporations are collecting people's personal information during 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, ostensibly 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 ensures that California's efforts to address the pandemic also maintain Californians' privacy.

AB 1782 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. *See* Sec. 1924(b); Sec. 1924.1(a). Even after consent is granted, TACT operators must provide a simple means for a user to revoke

---

[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.

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.

It is especially important to protect the privacy rights of employees by requiring their consent to TACT and prohibiting discrimination against employees that withhold consent. In many workplaces, employers may be insensitive to employees' privacy and other needs, yet employers have disproportionate power to require employees to submit to surveillance. To be effective, TACT programs require user buy-in, which requires informed consent. Without consent, workers might undermine the effectiveness of a coercive TACT program by putting their phones in airplane mode or leaving them at home. Additionally, one in five Americans do not have a smart phone, so a workplace mandate to submit to TACT could unfairly separate lower-income workers from their jobs. AB 1782 further protects employees by not limiting employers' ability to implement other health programs, including manual contact tracing, social distancing, masking, and voluntary TACT.

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. There is also a 60-day deadline to delete TACT-related data, with an exception for specified research. *See* Sec. 1924.1(f).

Sixth, public health entities cannot offer TACT systems that process geolocation information. *See* Sec. 104000(e). Existing geolocation tracking systems (GPS and cell site location information) are not accurate enough to know whether two people were close enough together to transmit the virus (six feet). But they are accurate enough to expose whether a person went to a hospital, protest, church, or theater.

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

Seventh, 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).

The bill empowers members of the public to enforce these rules. It also allows enforcement by the Attorney General, a district attorney, and a city attorney. *See* Sec. 1924.8.

These are important rules and enforcement mechanisms, and so we support this bill in its current form.

* * *

Again, we thank you for your leadership in carrying AB 1782, which contains important safeguards for TACT and COVID-related personal information. We are pleased to support this bill.

Sincerely,

Adam Schwartz
Senior Staff Attorney
Electronic Frontier Foundation

Becca Cramer-Mowder
Legislative Coordinator & Advocate
ACLU of California

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

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

Meghan Land
Executive Director
Privacy Rights Clearinghouse

Alegra Howard
Policy Advocate
Consumer Action

cc: Senate Appropriations Committee