July 27, 2020

Assembly Member Marc Levine
State Capitol
P.O. Box 942849
Room 5135
Sacramento, CA 94249-0010

Re: AB 660 on COVID-19 privacy – support if amend

Dear Asm. Levine:

We are five organizations dedicated to protecting consumer privacy. We write to thank you for your leadership in authoring AB 660. This legislation would help protect the data privacy of people in California whose personal information is processed for purposes of containing the COVID-19 outbreak. This bill is a good first step. We would be pleased to support it if amended to more fully protect the privacy of COVID-related data, as set forth below.

1. California needs COVID-19 privacy legislation.

Many government agencies and corporations are collecting our personal information to respond to the COVID-19 crisis. States are conducting manual contact tracing, often contracting with businesses to build new data management systems.[1] States also are partnering with businesses to create websites where we provide our health and other information to obtain screening for COVID-19 testing and treatment.[2] The federal government is sharing COVID-19 tracking data with its own corporate contractors, including TeleTracking Technologies[3] and Palantir.[4]

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

2 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.

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

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

There are many ways to misuse our COVID-related data. Some restaurants are collecting contact information from patrons to notify them later of any infection risk;[5] disturbingly but not surprisingly,[6] in at least one reported case a restaurant employee used a patron's information to send them multiple harassing messages.[7] Companies might divert our COVID data to advertising.[8] All this data might be stolen by identify thieves, stalkers, and foreign nations.[9]

Moreover, public health officials and their corporate contractors might share our COVID-related data with police and immigration officials.[10] This would frustrate containment of the outbreak, because many people will share less of their personal information if they fear the government will use it against them. Yet in some California communities, law enforcement officials themselves are conducting contact tracing.[11] Likewise, in many communities, police are demanding access to public health data about the residences of people who have been infected.[12] And now the federal government is proposing deployment of the National Guard to hospitals to process our COVID-related personal data.[13]

Unfortunately, existing data privacy laws do not adequately protect us from misuse of our COVID-related data. For example, federal HIPAA protections of health data apply only to narrowly defined healthcare providers and their business associations.[14] This is just one of many illustrations of why we need comprehensive consumer data privacy legislation.[15] Unfortunately, we don't have it.

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

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

[6] 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/.

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

[8] 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.

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

[10] https://www.eff.org/deeplinks/2020/04/telling-police-where-people-covid-19-live-erodes-public-health; https://www.scientificamerican.com/article/confirmed-the-us-census-b/

[11] https://www.fresnobee.com/news/local/article243795537.html.

[12] https://www.eff.org/deeplinks/2020/04/telling-police-where-people-covid-19-live-erodes-public-health.

[13] https://www.washingtonpost.com/health/2020/07/13/trump-administration-recommend-national-guard-an-option-help-hospitals-report-covid-19-data/; https://twitter.com/EFF/status/1283582883328741377.

[14] https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

[15] 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.

2. AB 660 would help protect COVID-19 privacy.

First, this bill would prohibit the sharing of contact tracing data with any entity other than a public health entity.

This disclosure limit is an important privacy protection. If a company collects a person's personal data while acting as a government contractor for contact tracing purposes, AB 660 would stop that company from selling that person's information to a data aggregator. And if a public health agency collects the same data, AB 660 would stop them from transferring it to police or immigration officials.

Second, the bill would prohibit law enforcement officials from engaging in contact tracing. This bar on the entanglement of police with public health is necessary to ensure that people cooperate with contact tracing. Absent this safeguard, people are likely to withhold information that is necessary to contain the outbreak.

3. AB 660 should be strengthened.

While AB 660 is a good start, California should do much more to protect our COVID-related data privacy.

First, we need a general rule of ***data minimization*** applicable to all aspects of our COVID-related data. We suggest the following: "A public health entity engaged in contact tracing, and any private entity contracting with a public health entity for this purpose, shall not collect, retain, use, or disclose data except as necessary and proportionate to control the spread of COVID-19." Under AB 660, a corporate contractor conducting contact tracing for a public health entity would remain free to *collect* far more personal data than actually needed for contact tracing, *retain* this data forever, and then *use* this data for targeted ads or other commercial purposes. AB 660 only limits the *disclosure* of this data. To do the most to prevent such monetization of our COVID-related data, California legislation should also provide: "A 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."

Second, we need a requirement of ***opt-in consent*** from a person before processing of their COVID-related data. We suggest the following: "A public health entity engaged in contact tracing, and any private entity contracting with a public health entity for this purpose, shall not collect, retain, use, or share data except with the informed opt-in consent of the data subject." Every person should be free to autonomously decide whether to share their personal data. This isn't just a matter of human rights. It is also a matter of public health: people will not cooperate with public health authorities absent trust, and unconsented privacy intrusions degrade trust. Relatedly, we need to empower people to revoke consent and swiftly purge their already-collected data.

Third, we need a requirement to ***purge stale data***. We suggest the following: "A public health entity engaged in contact tracing, and any private entity contracting with a public health entity for this purpose, shall purge all data collected for purposes of contact tracing within 30 days of the time of collection." COVID-19 has a 14-day incubation period.[16] Older information will not assist with contact tracing. But it can be stolen by data thieves, misused by agency employees, and deployed to now-unforeseen purposes by agency leaders. We would not object to a narrowly-crafted exception from this purge rule for a limited amount of aggregated and de-identified demographic data (such as race and ethnicity) 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 of this highly sensitive data.[17]

Fourth, we need a right to ***access, correct, and delete*** our COVID-related data. We suggest the following: "A person who discloses their data to a public health entity, or its contractor, for purposes of contact tracing shall have the rights to access, correct, and delete that data." These are standard features of data privacy laws, including (as to access and deletion) the California Consumer Privacy Act.[18]

Fifth, 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 health entity, or private contractor of a public health entity, 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 violation, and reasonable attorney fees." This is a standard feature of legislation that protects people from governmental and corporate wrongdoing.[19]

Sixth, the prohibition against contact tracing by law enforcement should include state as well as local law enforcement. We suggest amending the definition of "law enforcement official" by replacing all instances of "local agency" with "local ***or state*** agency."

* * *

Again, we thank you for your leadership in carrying AB 660, which is a good first step towards crafting legislation to protect COVID-related data privacy. We look forward to supporting AB 660 if it is amended as discussed above.

Sincerely,

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

[17] https://www.eff.org/deeplinks/2020/04/how-protect-privacy-when-aggregating-location-data-fight-covid-19.

[18] https://theccpa.org/.

[19] https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy.

Adam Schwartz
Senior Staff Attorney
Electronic Frontier Foundation

Kevin Baker
Director of Legislative Affairs
American Civil Liberties Union of California

Emory Roane
Policy Counsel
Privacy Rights Clearinghouse

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

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

cc. Members and staff, Senate Committee on the Judiciary