August 4, 2020

Senator Steven M. Glazer
Chair
State Capitol, Room 5108
Sacramento, CA 95814

Senator Ling Ling Chang
Vice Chair
State Capitol, Room 4062
Sacramento, CA 95814

Re: California A.B. 2004 (Calderon) re digital verified credentials of COVID-19 test results - OPPOSE

Dear Sen. Glazer and Sen. Chang:

We oppose A.B. 2004, which would authorize issuers of COVID-19 test results to do so with digital verifiable credentials. This bill is a blockchain solution in search of a problem and a thinly veiled attempt to cloak legislation endorsing a business model as a COVID-19 response. As explained below, the bill would (1) take us a step towards national digital identification, (2) create information security risks, (3) exacerbate social inequities in access to smartphones and COVID-19 tests, and (4) not effectively advance the bill's stated goals.

The bill

A.B. 2004, as amended on June 29, requires a state board to "establish a pilot program to explore methods of using verifiable health credentials for communication of COVID-19 test results or other medical test results in this state." *See* Sec. 2029(b). The bill defines "verifiable health credential" as "a portable electronic patient record issued by an authorized health care provider to a patient … , for which the authenticity of the record can be independently verified cryptographically." *See* Sec. 2029(a)(1).

One of the bill's findings identifies "the Verifiable Credentials Data Model developed by the World Wide Web Consortium (W3C)" as an example of a "cryptography-based verifiable credential model." *See* Sec. 1(c). The W3C

published its "Verifiable Credentials Data Model 1.0" in November 2019.[1] It identifies "distributed ledgers" as one example of "verifiable data registries."

The bill also vests the Department of Consumer Affairs with "sole jurisdiction over the authorization of health care providers for the issuing of verifiable health credentials pursuant to the pilot program," and requires that Department to "establish procedures for the authorization of issuers of verifiable credentials, including developing and maintaining a verifiable issuer registry." *See* Sec. 2029(e)(1).

A fact sheet for the bill identifies three potential uses of digital verifiable credentials of COVID-19 test results: (1) to provide "proof" of "immunization status"; (2) to provide proof of "medical test results" generally, in order to facilitate "traveling to a foreign country, sending children to school, [and] authorization to work with at-risk populations"; and (3) to encourage Californians to use "contact tracing applications." The fact sheet also states: "Verifiable credentials use blockchain technology to provide a credible solution to tracking and tracing data while protecting people's data and privacy."

The May 5 bill analysis states that the "purpose of the bill" is to "authorize the use of blockchain-based technology to provide verifiable credentials for medical test results, including COVID-19 antibody tests …" The analysis states that the bill's author wrote that such credentials could be used for "returning to work, travel or any other processes wherein verification of a COVID-19 test would be needed." The analysis also states that such credentials could be used as "'immunity certificates' for antibody tests in order to resume economic activity …" The May 31 and June 5 bill analyses likewise emphasize blockchain as a form of verifiable credential, and the use of such credentials during the pandemic to screen people for admission to "work, travel or any other processes."[2]

[1] https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.
[2] https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB2004.

Our objections

1. The bill would take us a step towards national digital identification.

We have long-opposed mandatory national identification systems.[3] As used today in numerous countries, these schemes typically assign an identification number to each person, who must use it for a broad range of identification purposes. Large amounts of personal information are linked to the identification number and stored in a centralized database. These schemes facilitate government surveillance of all occasions when people use their identification. The requirement to produce identity cards or numbers on demand habituates people into participating in their own surveillance.

Thus, we oppose the federal "Real ID" law, which creates a vast federal database linking together state-issued identifications.[4] Likewise, we are troubled by digital driver's licenses, among other reasons because they might be used to aggregate data about all the occasions when people use their driver's license as identification.[5]

Obviously, a system of blockchain-based verified credentials would have important differences from the national identification and digital driver's license schemes discussed above, because blockchain is a decentralized public ledger. Still, blockchain-based verified credentials would habituate people to present a digital token as a condition precedent to obtaining access to a physical space, and habituate gatekeepers to demand such digital tokens. Such a system could be expanded to document not just a medical test result, but also every occasion when the subject presents that result to a gatekeeper. It could also be expanded to serve as a verified credential of other pieces of personal information, such as age, pregnancy, or HIV status. And it is further troubling that all of that personal information associated with a blockchain verified credential could be linked to other digital record-keeping systems.

[3] https://www.eff.org/issues/national-ids.
[4] https://www.eff.org/issues/real-id.
[5] https://apnews.com/3db24f145e3a5f8f69f895bc12ddf2db; https://www.daily-journal.com/news/local/illinois-ponders-digital-driver-s-license/article_bae821ab-5a0d-5209-81f3-4b248144c795.html; https://www.huffpost.com/entry/could-plastic-drivers-licenses-become-a-thing-of-the_b_5bf41780e4b09851702fe10e.

2. The bill would create information security risks.

There are substantial information security hazards surrounding when a person presents a digital verifiable credential. If the digital credential is an image in the person's phone, then the person must unlock their phone to display it. This creates inherent risk that the phone could be physically seized and all of the personal information inside the unlocked phone examined. This risk is especially high if the credential is presented to a police officer or other government official.

Alternatively, the verified credential might be electronically transmitted from the person's phone to someone else's device. But such transmission would create a new threat vector for adversaries to surveil or steal both the transmitted credential and potentially information inside the person's phone.

3. The bill would exacerbate social inequities in access to smartphones and COVID-19 tests.

A smartphone-based system of digital verified credentials of COVID-19 test results would aggravate existing social inequities. About one-in-five people in the United States do not have a smartphone, according to a Pew Research Center study in 2019.[6] The smartphone "have-nots" include 47% of people who are 65 or older, 34% of people who did not graduate from high school, 29% of people who earn less than $30,000 per year, and 29% of people living in rural areas. Moreover, there are racial and ethnic inequities in access to COVID-19 testing,[7] among other inequities in access to COVID-19 health care.[8]

Thus, if our society deploys smartphone-based verification credentials of COVID-19 test results as the primary system to control access to public spaces like offices and schools, that would aggravate existing inequities in access to both smartphones and COVID-19 testing.

4. The bill would not effectively advance its stated goals.

When government proposes to use a technology in the name of solving a problem, in a way that creates risks, we must ask: has the government shown

6 https://www.pewresearch.org/internet/fact-sheet/mobile/.
7 https://www.chcf.org/blog/striving-equity-covid-19-testing/.
8 https://naacp.org/wp-content/uploads/2020/04/Coronavirus-Equity-Considerations.pdf.

the technology would be effective at solving the problem?[9] If not, the risks are not justified. Here, the proponents of digital verified credentials of COVID-19 test results have not shown that this technology would help address the outbreak.

First, there is an inherent problem with using verified credentials for the results of any medical test involving COVID-19: while the credentials might establish that a particular person received a particular result from a particular test, the credentials cannot establish the validity of the underlying test. Any negative test result for the presence of the virus can be a false negative, meaning the test subject has the virus but the test erroneously reports they do not.[10] Some COVID-19 tests have a false negative rate of as high 15%.[11] A verified credential of a negative test result implies "this person does not have COVID-19," but a negative test result actually means only "this person *probably* does not have it."

Second, one of the bill's stated goals is to establish digital verified credentials showing whether a person is immune from COVID-19. But no immunity test exists. As the World Health Organization concluded: "There is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection."[12]

Third, one of the bill's stated goals is to establish digital verified credentials for purposes of screening people for entry to public places, based on whether or not they present a health threat to others. But blockchain and COVID-19 infectiousness testing are a bad fit. Per the recommendation of California's Blockchain Working group, the "most critical question" when considering whether blockchain is an appropriate solution to a problem is to ask whether a permanent record is warranted, and to ensure that an unalterable record is neither superfluous or counterproductive.[13] This is in keeping with other recommendations about appropriate applications of digital verified credentials. While digital verified credentials might be suited to facts that are highly static (such as whether a person is 21 years old), they are poorly

9 https://www.eff.org/deeplinks/2020/04/how-eff-evaluates-government-demands-new-surveillance-powers.

10 https://www.cdc.gov/coronavirus/2019-ncov/downloads/Factsheet-for-Patients-2019-nCoV.pdf.

11 https://www.npr.org/sections/health-shots/2020/04/21/838794281/study-raises-questions-about-false-negatives-from-quick-covid-19-test.

12 https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19.

13 https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf

suited to facts that commonly change over time (such as whether a person is pregnant). Indeed, the abstract of the W3C's Data Model provides use cases that are highly static: whether a person has obtained a driver's license, a university degree, or a passport.

Here, on the other hand, digital verified credentials of negative virus test results would only show non-infectiousness at an earlier point in time, potentially days or weeks before a person presents their credentials to a gatekeeper. In the meantime, the person might have been infected. Worse, the immutability of the blockchain might allow that person to continue to present gatekeepers with test results showing non-infectiousness—even after a subsequent test shows infectiousness.

Fourth, one of the bill's stated goals is to encourage people to use contact tracing apps. But in the ascendant versions of such apps in the United States, such as the Apple-Google Bluetooth-based "exposure notification" system, people only share ephemeral identifiers with each other's phones and sometimes with a shared server, and never share medical test results with either.[14] Likewise, while a testing authority may give an infected person a credential that allows them to upload their ephemeral identifiers to the shared server, the testing authority does not share that person's test results with anyone. In short, contact tracing apps in the United States should not and generally will not involve the transfer of medical test results. So, there is no reason that a new system of verified credentials of test results would encourage a person to download a contact tracing app.

* * *

Thank you for considering our objection to A.B. 2004. We respectfully urge you to vote against this bill. We would be pleased to discuss this bill with you further.

Sincerely,

Adam Schwartz
Senior Staff Lawyer
Electronic Frontier Foundation
adam@eff.org

Becca Cramer-Mowder
Legislative Coordinator & Advocate
ACLU of California
bcramer@acluca.org

[14] https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf.