May 13, 2020

Majority Leader Ian Calderon
California State Assembly

Alexandra Medina
Blockchain Advocacy Coalition
ally@blockadvocacy.org

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

Dear Majority Leader Calderon and Ms. Medina:

We write to continue our recent discussions regarding A.B. 2004. We appreciate the conversation and your willingness to hear our concerns with this bill, and hope this discussion will continue.

However, we must oppose A.B. 2004, which would authorize the issuers of COVID-19 test results to do so with digital verifiable credentials. 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, (4) endorse one solution to an evolving technological problem, (5) fail to limit who may view credentials of test results, and (6) not effectively advance the bill's stated goals.

The bill

A.B. 2004, as amended for its May 5 hearing, provides: "An issuer, including an issuer that is a public entity, of COVID-19 test results or other medical test results may use verifiable credentials, as defined by the World Wide Web Consortium (W3C), for the purpose of providing test results to individuals."[1] The bill also provides that such verifiable credentials "shall follow the open source … W3C Verifiable Credentials Data Model," including three of its specifications: (1) Decentralized identifiers; (2)

[1] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB2004.

Verifiable credentials, and (3) JavaScript Object Notation for Linked Data (JSON-LD).

The W3C published its "Verifiable Credentials Data Model 1.0" in November 2019.[2] It identifies "distributed ledgers" as one example of "verifiable data registries."

The bill's fact sheet 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 official "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 states that such credentials could be used as "'immunity certificates' for antibody tests in order to resume economic activity …"[3]

Our concerns

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

We have long opposed mandatory national identification systems.[4] 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

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

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.[5] 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.[6]

Obviously, a system of blockchain 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 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 presented that result to a gatekeeper. It could also be expanded to serve as a verified credential of any other bit of personal information that might be relevant to a gatekeeper, such as age, pregnancy, or HIV status. And all of the personal information associated with a blockchain verified credential could be linked to other digital record-keeping systems.

2. The bill would create information security risks upon presentment of a digital credential.

We also have information security concerns surrounding the moment when a person presents their digital verifiable credential to a gatekeeper. If the digital credential is an image in the person's phone, then the person must unlock their phone to show it to the gatekeeper. This creates inherent risk that the gatekeeper will physically seize the phone, and examine or even copy all of the personal information inside the unlocked phone. This risk is especially high if the gatekeeper is a police officer or other government official.

---

[5] https://www.eff.org/issues/real-id.

[6] 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.

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

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

We have social equity concerns about a smartphone-based system of digital verified credentials of COVID-19 test results. About one-in-five people in the United States do not have a smartphone, according to a Pew Research Center study in 2019.[7] 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,[8] among other inequities in access to COVID-19 health care.[9]

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 endorses a single way to solve a technological problem.

Technologies often change faster than laws, and unpredictably so. As a result, today's sensible-seeming rule can easily become tomorrow's security weak point. So legislators should avoid endorsing one technological approach while discouraging others.

Unfortunately, A.B. 2004 endorses one approach for developers in California who seek to build digital verified credentials of medical test results. Although the W3C's Verifiable Credentials Data Model is not itself a limit on technological development, A.B. 2004 amounts to one, by singling out a particular verifiable-credential scheme as the favored approach. The bill thus disfavors other possible data delivery and storage solutions.

---

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

5. The bill does not limit who may view a verified credential.

A.B. 2004 authorizes the issuers of medical test results to do so with verifiable credentials. But it does not limit to whom such results may be issued, or upon who's authority. It is not clear how the bill would interact with existing medical privacy laws like HIPAA and California's Confidentiality of Medical Information Act. And according to the W3C Model on which the bill is built: "The persistence of digital information, and the ease with which disparate sources of digital data can be collected and correlated, comprise a privacy concern that the use of verifiable and easily machine-readable credentials threatens to make worse."[10]

Thus, the bill is a blank check to issuers to disseminate a verified credential, without first obtaining consent from the subject of that credential.

6. 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 can burden our freedoms, we must ask: has the government shown the technology would be effective at solving the problem?[11] If not, the burdens on our freedoms 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.[12] Some COVID-19 tests have a false negative rate of as high 15%.[13] 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."

---

[10] https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials.

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

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

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

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 recently concluded: "There is currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection."[14]

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. Perhaps the bill is oriented not just towards COVID-19 antibody immunity testing, but also towards COVID-19 infectiousness testing. But 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 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.[15] 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.

---

[14] https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19.
[15] https://blog.google/documents/73/Exposure_Notification_-_FAQ_v1.1.pdf.

* * *

Thank you for considering our concerns about A.B. 2004. We respectfully request that you withdraw 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