Date of Hearing: May 5, 2020

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 2004 (Calderon) – As Amended March 12, 2020

AS PROPOSED TO BE AMENDED

SUBJECT: Verifiable credentials: medical test results

SUMMARY: This bill would permit an issuer of COVID-19 test results or other test results to use verifiable credentials, as defined by the World Wide Web Consortium (W3C), for the purpose of providing test results to individuals. The bill would also require that verifiable credentials issued for this purpose follow the open source W3C Verifiable Credentials Data Model, including incorporation of decentralized identifiers, verifiable credentials, and JavaScript Object Notation for Linked Data (JSON-LD).

EXISTING LAW:

1) Specifies, under the federal Health Insurance Portability and Accountability Act (HIPAA), privacy protections for patients' protected health information and generally provides that a covered entity, as defined (health plan, health care provider, and health care clearing house), may not use or disclose protected health information except as specified or as authorized by the patient in writing. (45 C.F.R. Sec. 164.500 et seq.)

2) Provides, under the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const. art. I, Sec. 1.)

3) Prohibits, under the Confidentiality of Medical Information Act (CMIA), providers of health care, health care service plans, or contractors, as defined, from sharing medical information without the patient's written authorization, subject to certain exceptions. (Civ. Code Sec. 56 et seq.)

4) Defines "medical information" to mean any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. CMIA defines "individually identifiable" to mean that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. (Civ. Code Sec. 56.05(g).)

5) Provides that any business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or the provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis of treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of the CMIA. (Civ. Code Sec. 56.06(a).)

6) Requires an electronic health record system or electronic medical record system to protect and preserve the integrity of electronic medical information, to automatically record and preserve any change or deletion of any electronically stored medical information, including the identity of the person who accessed and changed the medical information, the date and time the medical information was accessed, and the change that was made. (Civ. Code Sec. 56.101(b)(1).)

7) Provides that any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of written or electronic medical records shall be subject to damages in a civil action or an administrative fine, as specified. (Civ. Code Sec. 56.36.)

8) Requires a health care professional at whose request a test is performed to provide the results of a clinical laboratory test to the patient if so requested by the patient, in oral or written form, in plain language, and provides that the health care professional may only disclose the results in electronic form if requested by the patient and if deemed most appropriate by the health care professional who requested the test. (Health & Saf. Code Sec. 123148(a).)

9) Provides that the electronic disclosure of test results shall be in accordance with any applicable federal law governing privacy and security of electronic personal health records, and that any state statute that governs privacy and security of electronic personal health records shall apply to test results and shall prevail over federal law if federal law permits. (Health & Saf. Code Sec. 123148(d).)

10) Defines "electronic health record" or "electronic medical record" to mean an electronic record of health-related information on an individual that is created gathered, managed, and consulted by authorized health care clinicians and staff. (Civ. Code Sec. 56.101(c); 42 U.S.C. Sec. 17921(5).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to introduce and authorize the use of blockchain-based technology to provide verifiable credentials for medical test results, including COVID-19 antibody tests, in order to improve the privacy and security of patient health records. This bill is sponsored by the Blockchain Advocacy Coalition.

2) **Author's Statement of Criticality**: In response to the unique constraints the COVID-19 crisis has placed on the legislative process, this Committee elected to focus attention this session on bills that address only the most urgent issues and issues critical for an efficient recovery from the pandemic. In order to prioritize bills that require immediate attention, the Committee asked the author of each bill to provide a Statement of Criticality explaining the applicability of one or more of the following criteria to that bill:

   - the bill addresses a problem that was created by, or has been significantly exacerbated by, the ongoing public health crisis due to COVID-19, or the response thereto;

   - the bill addresses an urgent problem that presents a threat to the safety and security of Californians and must be resolved immediately; or

- the bill makes a technical change to an existing program or function that must be immediately adopted to preserve the utility of that program or function.

In response, the Author writes:

> This bill is needed to provide an avenue for healthcare workers and individuals in our communities through which COVID-19 tests can be verified for any purpose – whether it be returning to work, travel or any other processes wherein verification of a COVID-19 test would be needed. Verifiable credentials provide a way to do this, but existing law does not provide any minimum standards for what constitutes a verifiable credential. This bill would provide those minimum standards, as well as give doctors the legal confidence that these credentials are a trusted and secure way to provide test results to individuals, while giving individuals assurance that their privacy will be protected.
>
> There is a strong need to provide a testing and tracking program that individuals feel comfortable participating in. In a recent poll by Washington Post-University of Maryland, it was reported that approximately 3 in 5 Americans are unable or unwilling to use the infection-alert system being developed by large technology companies. Conversely, current research from Covid Watch, a Stanford University research project, suggests that around 60 [percent] of a population needs to engage with a contact tracing program for it to be successful. Covid Watch's white paper emphasizes the need for community engagement in a tracking/tracing program. This bill is needed to bring these numbers closer to one another by providing a privacy-protected way of participating in such a program. (Internal citations omitted.)

The Committee agrees that the issues addressed by this bill are timely and critical under the current circumstances. Establishing a secure and privacy protective mechanism for communicating COVID-19 test results that can be accessed at will by the subject of the test would obviate the need for traditional "immunity certificates," as have been suggested for resumption of economic activity while recovering from the COVID-19 crisis. This bill aims to authorize a mechanism alleging these characteristics.

3) **Blockchain, generally**: As society has evolved, so too has trade and society's reliance on institutions to facilitate trade between individuals who may not know one another or even be located near one another. When consumers use "eBay," "Amazon," etc., they are effectively using digital marketplaces and platforms that help facilitate an exchange of value. Blockchain is a network that allows individuals to conduct transactions, "peer-to-peer," with fewer (or no) intermediaries (i.e., middle men, such as banks, clearing houses, payment networks). In place of those traditional intermediaries or institutions, blockchain relies on a software code run by different computers that are guaranteeing these transactions as they happen. The Massachusetts Institute of Technology (MIT) Technology Review describes blockchain as "a decentralized, online record-keeping system, or ledger, maintained by a network of computers that verify and record transactions using established cryptographic tecniques." Notably, the ledger of transactions can be added to, but never erased from. In other words, the data that has been added to the ledger, can never be changed. It does all this though a mechanism for creating consensus between scattered or distributed parties that do not need to otherwise trust each other, but need to trust the mechanism by which their consensus is established. It is, in so many words, a decentralized, transparent, immutable, append-only, cryptography-transmitted, digital, distributed public ledger. (Svikhart,

Blockchain's Biggest Hurdle (Nov. 2017) <https://www.stanfordlawreview.org/online/blockchains-big-hurdle/> [as of May 4, 2020].)

4) **Blockchain uses**: Blockchain initially gained notoriety for its applications in facilitating transactions using decentralized, digital currencies known as cryptocurrencies (e.g. Bitcoin, Ethereum). Recording financial transactions, however, is just one of blockchain's many applications. Blockchain technology "can maintain accurate chains of title to securities and other legal instruments in a reliable electronic form" and has been identified as having incredible value in its potential to record and secure an immense volume of trades and financial transactions on a perpetual basis. (Svikhart.) According to a 2016 report by the Vermont Secretary of State, a valid blockchain can reliably confirm a party submitting a record to the blockchain, the time and date of the submission, and the contents of the record at the time of submission. This means blockchain holds significant utility for confirming authenticity of records, including validation that the record has not been doctored.

   Recently, public and private entities alike have shown interest in blockchain as a possible mechanism for digital record keeping. In 2018, Governor Brown signed into law two bills relating to blockchain technology, signaling the California state government's interest in exploring applications of blockchain. AB 2658 (Calderon, Ch. 875, Stats. 2018) in particular set the stage for future public and private adoption of blockchain technology by establishing a taskforce to evaluate the uses of blockchain in California's businesses and government. This taskforce is expected to report its findings to the Legislature by July 1, 2020.

   What makes blockchain so attractive for many uses is its security. "Blockchains, like Bitcoin and Ethereum, have not yet been hacked. They are considered to be very secure. It is very challenging, almost impossible, to change any transaction information once it is validated and becomes part of a block." (Svikhart.) This security appears to be built into blockchain's very structure, "where each block is linked to another block [. . .] in a time-stamped chronological order. [Thus, to] access data of the first ever created block, you have to traverse from the last created block, then the block before that, so on and so forth till you reach the first block. Each block contains elements like the version # [hash], reference of the address of the previous block, timestamp, transactional data, block size etc." (Vaidya, Medium, *Decoding the Enigma of Blockchain* (Nov. 28, 2016) <https://medium.com/all-things-ledger/decoding-the-enigma-of-blockchain-e0861fcab4b7> [as of May 4, 2020].) As a result, corruption or hacking of blockchain transactions are made incredibly unlikely, if not impossible given that the hacker would have to manipulate each block starting from the latest block added to the network in order to corrupt or hack any single transaction of a certain block.

5) **Verifiable credentials:** Verifiable credentials are one promising application of blockchain technology that permits the certification of official documents by authorized issuers, in order to give the individual control over their own confidential information. The W3C, in its "Verifiable Credentials Data Model 1.0," defines a verifiable credential as "a tamper-evident credential that has authorship that can be cryptographically verified." In essence, a verifiable credential is a set of claims issued about a subject for which the issuer of those claims can be independently verified. In practice, this means a credential describing some information about an individual, e.g. the individual's age, is issued by an issuer, e.g. the DMV, who has been authorized to confer these credentials. The individual can then present that credential to another entity, e.g. a liquor store, who can cryptographically verify through a data registry that the issuer was authorized to provide that credential. In the examples provided, rather

than presenting a physical driver's license in order to purchase alcohol, the liquor store could verify that the individual is over the legal drinking age by, with the consent of the individual, viewing the digital credential, and then verifying that it was issued by a legitimate, authorized entity, confirming the ID is not fake.

This technology has been suggested by many to have particular utility in the healthcare space, by permitting individuals to have ready access to their personal health records, and providing a mechanism for verifying prescriptions. As discussions of "immunity certificates" for antibody tests in order to resume economic activity in response to the COVID-19 crisis, application of this technology seems particularly timely. Presumably, this would involve an individual receiving a COVID-19 antibody test, by a health professional, authorized by a public health agency to confer health credentials, issuing a credential certifying the results of that test, and then the person requiring certification of test results (e.g. employer, other health professional) verifying that the credential was legitimately issued.

6) **The W3C Verifiable Credentials Data Model, privacy, and security**: While incredibly secure because it is extremely difficult to hack, the W3C Recommendation, published November 19, 2019, cautions that there may be some privacy vulnerabilities inherent to the technology, and that careful and specifically tailored approaches to different use cases are necessary to avoid compromising confidential information. W3C writes:

> 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. (*See* <https://www.w3.org/TR/vc-data-model/> [as of May 4, 2020].)

The Recommendations identify 16 different potential privacy vulnerabilities and eight potential security vulnerabilities, suggesting certain best practices in response to each of them, depending on the demands of the use case. That these practices are use case dependent is a critical consideration, since generally relying on these recommendations as the basis for statute may result in inappropriate application of certain practices in the case of medical test result credentials, which are particularly sensitive and must be accessed by certain parties in certain ways. W3C, in the Model, notes:

> It is important to recognize there is a spectrum of privacy ranging from pseudonymous to strongly identified. Depending on the use case, people have different comfort levels about what information they are willing to provide and what information can be derived from what is provided.
>
> […]
>
> ***The Verifiable Credentials Data Model strives to support the full privacy spectrum and does not take philosophical positions on the correct level of anonymity for any specific transaction.*** The following sections provide guidance for implementers who want to avoid specific scenarios that are hostile to privacy. (Emphasis added.)

Notably, this bill provides no specificity in terms of the actual implementation of the guidance for this purpose, apart from requiring implementation to incorporate "decentralized identifiers," "verifiable credentials," and "JavaScript Object Notation for Linked Data

(JSON-LD)," none of which are associated in the bill with definitions or with specification of the manner of incorporation or interaction with one another. Though the bill mandates that credentials issued pursuant to its authorization must follow the W3C Verifiable Credentials Data Model, it is silent on which recommendations are included in the mandate. The recommendations included in the Model, including those to address privacy and security vulnerabilities, are constructed as suggestions that are dependent on specific use cases, making it unclear what precisely it means to follow this Model. This means the legal framework imposed, despite legitimizing the use of the technology, does not discernably specify a cautious approach comprised of specific guidelines for the use of this technology.

A legal framework codifying these recommendations would necessarily be fairly complex in order to assign incumbency to specific parties for certain aspects of privacy protective practices. The recommendations do not specify exact approaches, but rather suggest aspirations and ideals that a privacy-protective system should adopt. For example, "[t]he design of any verifiable credentials ecosystem…should strive to be as privacy-respecting as possible by preferring single-use verifiable credentials whenever possible." In order to produce legislation reliant on this recommendation, it is necessary for either the Legislature or an implementing agency to determine whether "whenever possible" is dictated by a certain threshold of feasibility, by what is commercially viable, by what is convenient for the patient, by what is convenient for the issuer, or by actual technical possibility. While a task force or agency could develop such guidelines or regulations to that end, doing so with due diligence would take significant time, hampering the immediate implementation of the technology this bill seeks to permit. The bill does not specify an implementing or overseeing agency, and this type of technology could reasonably fall within the purview of the Department of Technology, the Department of Public Health, or the Department of Health Care Services, all of whom are at the epicenter of the public health response to COVID-19.

The author notes that the bill will not "[burden] state agencies as it does not require them to adopt verifiable credentials – only provides them the ability to do so." Given the lack of clarity on what precisely this bill is authorizing, however, promulgating rules and regulations to make this framework workable would be necessary, and would require an enormous dedication of executive staff resources and agency funds, burdening the selfsame agencies upon which the COVID-19 crisis has primarily imposed.

Furthermore, though recommendations provided are intended to improve data privacy, some may come at the expense of workability, convenience, cost, or feasibility. A thorough analysis of the particular costs and benefits of each recommendation in the use case specified by this bill, i.e. the issuing of medical test results, is necessary to determine which recommendations from the W3C model, if any, should be codified, and in what manner. The exact language used in this case can have substantial repercussions for both workability and privacy, and should not be constructed hastily. Put simply, the W3C model was not designed to constitute a set of specific legal guardrails, but rather recommendations on best practices for implementing technology based on verifiable credentials. Relying on this model to substantiate this bill is thus likely to pose significant problems for clarity of obligations and implementation of oversight.

7) **Immutability of the blockchain may cause difficulty in light of the limited reliability of existing COVID-19 antibody tests**: Several proof-of-concept whitepapers, academic manuscripts, and prototypes have produced workable systems for the issuing and validation

of verifiable credentials for health information. For instance, a recent preprint of an academic manuscript posted to arXiv, an open science repository, detailed a prototype of a mobile phone application that employs verifiable credentials specifically for the purpose of certifying COVID-19 antibody test results for putatively immune individuals to resume work (Eisenstadt et al., *COVID-19 Antibody Test Certification There's an app for that*, (Apr. 2020) <https://arxiv.org/pdf/2004.07376> [as of May 4, 2020].) This prototype may indeed, as the paper suggests, be sufficiently vetted and developed for rapid deployment, but it should be noted that the value of reporting of COVID-19 antibody test results necessarily depends on resistance to the virus conferred by previous exposure, which has not been confirmed, and has been called into question by a recent World Health Organization (WHO) scientific brief:

> WHO continues to review the evidence on antibody responses to SARS-CoV-2 infection. Most of these studies show that people who have recovered from infection have antibodies to the virus. However as of 24 April 2020, no study has evaluated whether the presence of antibodies to SARS-CoV-2 confers immunity to subsequent infection by this virus in humans.
>
> Laboratory tests that detect antibodies to SARS-CoV-2 in people, including rapid immunodiagnostic tests, need further validation to determine their accuracy and reliability. Inaccurate immunodiagnostic tests may falsely categorize people in two ways. The first is that they may falsely label people who have been infected as negative, and the second is that people who have not been infected are falsely labelled as positive. Both errors have serious consequences and will affect control efforts. These tests also need to accurately distinguish between past infections from SARS-CoV-2 and those caused by the known set of six human coronaviruses. Four of these viruses cause the common cold and circulate widely. The remaining two are the viruses that cause Middle East Respiratory Syndrome and Severe Acute Respiratory Syndrome. People infected by any one of these viruses may produce antibodies that cross-react with antibodies produced in response to infection with SARS-CoV-2. (WHO, *"Immunity passports" in the context of COVID-19*, (Apr. 2020) <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19> [as of May 4, 2020].)

As such, the adoption of this technology for verifying these test results may be of limited utility for the immediate resumption of economic activity, which is likely the intention of this bill. Moreover, the limited reliability of COVID-19 antibody tests may pose additional issues in light of the immutability of the blockchain-based technology underlying verifiable credentials. A test result that is misread or that is invalidated by subsequent tests cannot be overwritten in the blockchain once verified, meaning the invalid result would nonetheless confer a verifiable credential from an authorized issuer that could be used to fraudulently resume employment or obtain public benefits, circumstances to which the author envisions this technology applying. In other words, explicit statutory authorization, and the legitimacy such attention confers, may be premature given current questions as to the value of this data.

8) **Existing law likely already permits the use of verifiable credentials for the purposes described**: As far as Committee staff can determine, current law does not prevent the use of "verifiable credentials," as defined, for the purpose of providing or verifying medical information, so long as that method of disclosure conforms to existing laws relating to authorization by the patient for the sharing of that information, and to the requirements for confidentiality already in place. Consequently, this bill has the potential to complicate and

confuse existing law with respect to the sharing of medical information, including COVID-19 and other medical test results. By providing explicit authorization in statute for a practice that could reasonably be understood to be permissible under current law, adopting the provisions of this bill would potentially create a legal presumption that the Legislature does not believe existing law already permits this practice. As a result, current use of verifiable credentials for communication and verification of COVID-19 or other medical test results, and their use at any point prior to January 1, 2021, could be viewed as legally impermissible, when this is not necessarily the case.

9) **It is unclear how this bill would interact with existing health information privacy laws, and whether existing confidentiality requirements apply**: Importantly, the bill lacks any specific standards for the use of verifiable credentials in issuing medical test results, making it unclear whether the process of issuing verifiable credentials must conform to existing confidentiality requirements for the communication of medical information, including those provided by the federal Health Insurance Portability and Accountability Act (HIPAA) and California's Confidentiality of Medical Information Act (CMIA). These health information privacy laws largely rely on a set of specific limitations on the disclosure of individual health information and requirements for the maintenance and communication of that information.

   Whether issuing or accessing a verifiable credential constitutes the communication of health information, and whether the blockchain maintaining metadata relating to this information constitutes storage of individual health data, remain open questions. In an effort to provide such standards, the author has added language that requires verifiable credentials issued for these purposes to follow "the open source World Wide Web Consortium (W3C) Verifiable Credentials Data Model, including incorporation of all of the following specifications as described therein: 1) decentralized identifiers; 2) verifiable credentials; 3) JavaScript Object Notation for Linked Data (JSON-LD)." However, these standards provide very little guidance on how this framework should be operationalized, including how these specifications interact, what they mean, and whether other specifications or recommendations from the W3C model must also be incorporated.

   Additionally, though California has implemented several laws to protect the privacy and integrity of electronic medical records, this bill calls into question whether verifiable credentials, an electronic avenue for verifying and communicating medical records, are bound by the same laws as other electronic medical records, because they are treated in this bill as separate and apart from existing policy relating to electronic medical records. Though there are potential privacy benefits to the use of cryptographic technologies, including verifiable credentials, for communicating health records if bound by sufficient standards and practices, this bill may actually compromise the privacy of these test records by arguably exempting them from the privacy protections the Legislature has already deemed essential for other electronic medical records.

10) **The bill relies on a dynamic, open-source document to provide definitions and specifications, which are liable to change without notice**: The bill itself fails to provide static definitions for any of the technical terms it includes, many of which refer to technical structures and processes that differ from the common usage of those terms. It is also problematic that the W3C Verifiable Credentials Data Model is an open source, living document that has gone through several iterations with more to come. The bill does not specify which draft of this model it is drawing definitions and implementation guidance

from, adding to its opacity. Throughout that process, the already highly interdependent definitions in the model may ultimately change or be removed, disrupting any workable framework the state had been able to implement in that time, and possibly even dramatically changing the practicalities of the law.

Protecting the privacy of our most sensitive personal data requires a well-developed, comprehensive set of standards and practices with redundant protections and clear specifications, in order to ensure such sensitive information does not fall into the wrong hands. That this bill includes "other medical test results" in addition to COVID-19 test results yields a substantial body of health information that could be compromised by imprudent implementation of this technology. The lack of static definitions for terms, the reliance on a dynamic, open-source model to comprise the legal framework, and the lack of guidance on how that model should be interpreted or implemented, makes this bill exceedingly vague, and raises the potential for catastrophic data security and privacy breaches.

11) **Author's amendments**: The above analysis is based on the following amendments offered by the author, rather than the bill in print.

1) On page 2, before line 1, insert:

SECTION 1. Title 1.81.7 (commencing with Section 1798.300) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.7. VERIFIABLE CREDENTIALS

1798.300. (a) 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.

(b) Verifiable credentials issued pursuant to subdivision (a) shall follow the open source World Wide Web Consortium (W3C) Verifiable Credentials Data Model, including incorporation of all of the following specifications as described therein:

(1) Decentralized identifiers;

(2) Verifiable credentials;

(3) JavaScript Object Notation for Linked Data (JSON-LD).

2) On page 2, strike out lines 1 to 37, inclusive, and strike out pages 3 to 9, inclusive

12) **Arguments in support**: In support of this bill, the Blockchain Advocacy Coalition, an organization advocating for "informed regulation of blockchain technology to help provide clear standards and direction to industries utilizing this cutting-edge technology" that is sponsoring the bill, argues:

If AB 2004 were to become law, a patient taking a COVID-19 antibody test could request a verifiable credential from their doctor. The doctor could verify the test results and send them to the patient. The doctor would store their records however they already do, and

the patient would have sole control over their test result. They could choose to share with an employer to re-enter the workforce, with the state to receive benefits, or with a barber to enter a salon. It's up to them. None of these parties could access their credential without their explicit consent. AB 2004 simply authorizes the use of VCs as a method of conveying medical test results and establishes stringent standards for an acceptable VC.

[…]

This bill is timely and vital because contact tracing has been listed as one of the six core indicators to re-open the economy. Research indicates at least 56% of the population needs to engage with a contract tracing program for it to be successful [but] public polling demonstrates that far fewer people are enthusiastic about sharing this data with the government.[…] Offering an alternative that allows individuals to control their own data is a vital step in broadening the demographics of who will participate in a contract trace system.

13) **Arguments in opposition**: In opposition to this bill, a coalition of civil liberties and digital privacy rights advocacy groups comprised of ACLU California, Center for Digital Democracy, Electronic Frontier Foundation, and Privacy Rights Clearinghouse argues:

We regret to inform you of our opposition to AB 2004 as it is proposed to be amended to give a blank check to issuers of medical tests to share test results with anyone with no more of a check than that person has verifiable credentials, as defined by the World Wide Web Consortium. By not limiting the sharing of test results beyond requiring that someone trying to access test results has verifiable credentials, the bill allows anyone with a verifiable credential to get anyone's else [*sic*] test results.

Additionally, the bill language is not clear on the scope of the testing, which private or public entities would be covered, and other questions that we were unable to ascertain answers to given the lateness of the proposed amendments.

14) **Prior legislation**: AB 2568 (Calderon, Ch. 875, Stats. 2018) *See* Comment 4.

SB 838 (Hertzberg, Ch.889, Stats. 2018) authorized corporations and social purpose corporations, which do not otherwise have outstanding securities traded on one of the major U.S. stock exchanges, to adopt provisions within their articles of incorporation authorizing certain records administered by or on behalf of the corporation to be recorded and kept on or by means of blockchain technology, as specified.

REGISTERED SUPPORT / OPPOSITION:

Support

Blockchain Advocacy Coalition (sponsor)

Oppose

ACLU of Northern California, Southern California, and San Diego and Imperial Counties
Center for Digital Democracy

Electronic Frontier Foundation
Privacy Rights Clearinghouse

Analysis Prepared by: Landon Klein / P. & C.P. / (916) 319-2200