SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2021-2022 Regular Session

AB 751 (Irwin)
Version: February 16, 2021
Hearing Date: July 13, 2021
Fiscal: Yes
Urgency: No
CK

SUBJECT

Vital records: certified copies: electronic requests

DIGEST

This bill makes permanent the current authorization of public officials to accept electronic requests for vital records using electronic verification of identity to authenticate the identity of the applicant. The bill further provides guidelines by which the verification shall be carried out, including authorization to use biometric comparison as a method of identity verification.

EXECUTIVE SUMMARY

The Office of Vital Records is charged with the responsibility of maintaining a uniform system for registration and a permanent central registry with a comprehensive and continuous index for all birth, death, fetal death, marriage, and dissolution certificates registered for vital events which occur in California. Certified copies of these records are available from the State Registrar, the 58 county recorders, and 61 local health jurisdictions.

Currently, the State Registrar, a local registrar, or a county recorder is authorized to furnish a certified copy of a birth, death, or marriage certificate to an authorized person, as defined, who submits a written, faxed, or digitized image of a request accompanied by a notarized statement, sworn under penalty of perjury, that the applicant is an authorized person. In addition, existing law authorizes these officials to accept an electronic request for a certified copy of these records if the request is accompanied by an electronic verification of identity and an electronic statement sworn under penalty of perjury. This additional authorization expires on January 1, 2022.

This bill deletes the January 1, 2022, sunset date, thereby applying those provisions indefinitely. It also specifies the guidelines for the electronic verification of identity and requires the completion of a privacy risk assessment, as required by those guidelines.

This bill is sponsored by the County Recorders Association of California. It is supported by several counties and TechNet. It is opposed by a number of consumer and privacy groups, including ACLU California Action and Oakland Privacy, who raise privacy and security concerns with the extended authorization.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Requires the State Registrar, local registrar, or county recorder ("public officials"), upon request and payment of the required fee, to supply to an applicant a certified copy of the record of a birth, fetal death, death, marriage, or marriage dissolution registered with the official. Public officials are only authorized to provide certified copies of birth, death, and marriage records only as authorized under Section 103526 or 103526.5 of the Health and Safety Code. (Health & Safety Code § 103525.)

2) Provides that when the original forms of certificates of live birth furnished by the State Registrar contain a printed section at the bottom containing medical and social data or labeled "Confidential Information for Public Health Use Only," that section shall not be reproduced in a certified copy of the record except as specifically authorized. (Health & Safety Code § 103525(a).)

3) Provides that if a public official receives a written, faxed, electronic, or digitized image of a request for a certified copy of a birth, death, or marriage record pursuant to Section 103525 that is accompanied by a notarized statement sworn under penalty of perjury, an electronic verification of identity accompanied by an electronic statement sworn under penalty of perjury, or a faxed copy or digitized image of a notarized statement sworn under penalty of perjury, that the applicant is an authorized person, as defined in this section, that official may furnish a certified copy to the applicant. (Health & Safety Code § 103526(a)(1).)

4) Requires a faxed or digitized image of the notary acknowledgment accompanying a faxed request received for a certified copy of a birth, death, or marriage record to be legible and, if the notary's seal is not photographically reproducible, to show specified information relating to the notary. If a request for a certified copy of a birth, death, or marriage record is made in person, the official shall take a statement sworn under penalty of perjury that the applicant is signing the applicant's own legal name and is an authorized person, and that official may then furnish a certified copy to the applicant. (Health & Safety Code § 103526(a)(2).)

5) Authorizes an official, if a request for a certified copy of a birth, death, or marriage record is made electronically, to accept an electronic verification

authenticating the identity of the applicant using a multilayered remote identity proofing process that complies with all of the following requirements:

a) meets or exceeds the National Institute of Standards and Technology (NIST) electronic authentication guideline for multilayered remote identity proofing;
b) verifies the applicant's valid government-issued identification number and financial or utility account number. This verification must occur through record checks with the state or local agency or a credit reporting agency or similar database and shall confirm that the name, date of birth, address, or other personal information in the record checks are consistent with the information provided by the applicant;
c) meets or exceeds the information security requirements of the Uniform Electronic Transactions Act (CalUETA), Civil Code section 1633.1 et seq., and other applicable state and federal laws and regulations, as provided, to protect the personal information of the applicant and guard against identity theft; and
d) retains for each electronic verification, as required by the NIST electronic authentication guideline, a record of the applicant whose identity has been verified and the steps taken to verify the identity. (Health & Safety Code § 103526(a)(3)(A).)

6) Requires, if an applicant's identity cannot be established electronically pursuant to the above, the applicant to include with their request a notarized statement of identity. (Health & Safety Code § 103526(a)(3)(B).)

7) Provides that, if the person requesting a certified copy of a birth, death, or nonconfidential marriage record is not an authorized person or is an authorized person who is otherwise unable to satisfy the above requirements, the certified copy provided to the applicant shall be an informational certified copy and shall display a legend that states "INFORMATIONAL, NOT A VALID DOCUMENT TO ESTABLISH IDENTITY." The legend shall be placed on the certificate in a manner that will not conceal information. (Health & Safety Code § 103526(b)(1).)

8) Sunsets the above provisions of Section 103526 on January 1, 2022, and makes effective the previously existing statute, which does not allow for electronic requests accompanied by an electronic verification of identity. (Health & Safety Code § 103526(h).)

This bill:

1) Removes the sunset date from Section 103526.

2) Amends the applicable standards to require the remote identity proofing process to comply with NIST Special Publication 800-63A Digital Identity Guidelines, or

its successor publication, on electronic authentication guidelines for multilayered remote identity proofing.

3) Requires the process to verify to Identity Assurance Level 2, as described within these guidelines.

4) Provides that the required verification may include record checks with the state or local agency, a credit reporting agency, or a similar database, knowledge-based verification, physical comparison, and biometric comparison.

5) Requires the public officials to complete a privacy risk assessment, as required by the NIST guidelines.

6) Repeals the version of Section 103526 set to take effect on January 1, 2022.

COMMENTS

1. Stated intent of the bill

According to the author:

> AB 751 makes permanent a program to request vital records online that has for over half a decade proven successful and valuable to Californians. 25 counties, including my home of Ventura County, have implemented remote identity proofing to access vital records, which has become invaluable in the midst of the pandemic. As we have learned this past year, it is imperative that government agencies have flexibility so they may continue to service constituents in a timely manner. Safe and convenient access to vital records is essential to Californians and this bill ensures that continues to be available in our state.
>
> California has also long been a leader in advancing technology and this bill continues to build that legacy. By adjusting the language to more faithfully reflect NIST standards, AB 751 ensures that California keeps pace with technological advances in identity proofing and keeps Californians' information secure.

The sponsor of the bill, County Recorders Association of California, writes:

> Since January 1, 2018, counties that have been utilizing a multilayered remote identity proofing process have been reporting that, approximately 80% of all customers are successful in having their identity authenticated by the process. This process has proved to reduce the time and cost to

> customers who are unable to visit the County Recorder's office in the county in which the life event occurred.
>
> The deleting of the sunset provision may give non-participating counties the confidence to enroll their counties into a system that provides a multilayered proofing process. This could afford a greater segment of the public to request and receive their vital record in a more effective and costly manner.

2. A brief history of privacy-protective vital record request laws

As discussed, the state maintains the system and registry for all birth, death, fetal death, marriage, and dissolution certificates registered for vital events which occur in California. Specified public officials at the state and local levels are required to supply, upon request and after payment of a required fee, applicants with certified copies of records of birth, fetal death, death, marriage, or marriage dissolution registered with the officials. Sections 103526 or 103526.5 of the Health and Safety Code provide the authorized manner by which these public officials are to provide certified copies of birth, death, and marriage records.

Two decades ago, it was revealed that California had sold the birth records of more than 24 million Californians to companies that then provided access to them on the internet. In response, the Senate Insurance Committee held an informational hearing demonstrating the ease with which identity thieves could obtain personal information about others. The hearing revealed that the State Registrar routinely sold electronic compilations of public record information to anyone who could pay for the records with no restrictions on their use. The records sold covered births from 1905 to 1995, and – "included names, birth dates, places of birth and mothers' maiden names, a key ingredient to accessing customer financial information at many banks and credit card companies."[1]

In order to prevent fraud and identity theft, the Legislature enacted a number of protective measures with regard to vital records in the wake of this incident. AB 247 (Speier, Ch. 914, Stats. 2002) and AB 1614 (Speier, Ch. 712, Stats. 2002) established controls for the release of, and access to, birth and death records. This included the creation of Section 103526, the statute being amended by this bill, which originally read:

> If the State Registrar, local registrar, or county recorder receives a written request for a certified copy of a birth or death record pursuant to Section 103525 that is accompanied by a notarized statement sworn under penalty

[1] Stefanie Olsen, *Identity crisis: Birth records online* (January 2, 2002) cnet, https://www.cnet.com/news/identity-crisis-birth-records-online/. All internet citations are current as of July 7, 2021.

> of perjury that the requester is an authorized person, as defined in this section, that official may furnish a certified copy to the applicant in accordance with Section 103525. If a request for a certified copy of a birth or death record is made in person, the official shall take a statement sworn under penalty of perjury that the requester is signing his or her own legal name and is an authorized person, and that official may then furnish a certified copy to the applicant.

AB 130 (Jeffries, Ch. 412, Stats. 2009) extended the existing limitations on release and access of birth and death records to marriage records in order to prevent the unauthorized use of personal information.

3. Loosening the requirements for vital record requests

After the series of statutes detailed above tightened the processes for requesting and receiving vital records, a new wave of bills began to provide more ready access. First, AB 464 (Daly, Ch. 78, Stats. 2013) updated the law regarding vital records to allow *digitized images* to be used, in addition to written or faxed documents, as part of a request for a certified copy of a vital record. The law still required these requests to be accompanied by a notarized statement, sworn under penalty of perjury, that the requester is an authorized person.

However, AB 2636 (Linder, Ch. 527, Stats. 2016) again updated the statute to allow public officials to accept electronic requests for these vital records. While the other methods required a statement sworn under penalty of perjury that the applicant is an authorized person to be notarized, the new electronic request need only be accompanied by an electronic sworn statement to that effect. This more flexible process was intended to address the backlogs and long waiting times that existed for vital record requests.

In connection with these electronic requests, AB 2636 authorized a public official to accept an electronic verification authenticating the identity of the applicant using a multilayered remote identity proofing process that complies with specified requirements. This includes meeting or exceeding the NIST electronic authentication guideline for multilayered remote identity proofing.

The process must verify the applicant's valid government-issued identification number and a financial or utility account number. This verification must occur through record checks with the state or local agency or a credit reporting agency or similar database and shall confirm that the name, date of birth, address, or other personal information in the record checks are consistent with the information provided by the applicant. The process must also meet or exceed the information security requirements laid out in federal and state law, as provided, and provide some protection for the personal information of the applicant and guard against identity theft.

According to this Committee's analysis of the bill, groups in opposition to AB 2636 argued that "privacy protections should not be set aside merely to facilitate the issuance of vital records." The opposition requested, and this Committee recommended, a sunset on the new provisions of the bill and a mechanism for acknowledging fraud alerts placed by persons who had experienced identity theft. Ultimately the bill did place a sunset, later extended to January 1, 2022, on the bill and required public officials that fulfilled electronic requests for vital records to report on their systems. This acknowledged the initial purpose of these laws, to prevent fraud and identity theft.

This bill removes that sunset date. A coalition of privacy groups in opposition urge that at most the sunset be pushed out and that better data be collected on how these new systems are working and whether there is an increased incidence of fraud and identity theft.

Opposition points to reports that indicate extremely high denial rates during the pilot of the program, which they argue could be indicative of attempted fraud. The author argues this simply shows the verification methods are working. Arguably, there is not enough evidence that this movement toward electronic requests is not without some security issues. Therefore, some consideration should be given to whether additional reporting may be called for or whether there should simply be an extension of the sunset date to ensure the Legislature revisits the issue to assess any concerns that manifest.

There are also concerns about this data being put to other uses beyond verification for the provision of vital records. In response, the author has agreed to the following amendment:

Amendment

Add: "Personal information and documents provided to the state Registrar, local registrar, or county recorder for the purpose of identity verification to acquire vital records shall not be used, shared, distributed or accessed by any other state or municipal agency or third party for any other purpose or purposes."

4. <u>Opening the door to new identity verification methods</u>

The bill also amends the verification processes to be used in connection with electronic requests. The new provisions require the process to meet or exceed NIST Special Publication 800-63A Digital Identity Guidelines, or its successor publication, on electronic authentication guidelines for multilayered remote identity proofing. The bill also explicitly authorizes verification to include record checks with credit reporting agencies, knowledge-based verification, physical comparison, and biometric comparison.

Writing in opposition, a coalition of privacy and consumer advocacy groups highlight serious privacy concerns with the new verification methods authorized by this bill:

> AB 751's methods for identity verification present troubling privacy implications for all Californians. There are far too many inherent risks in verifying someone's identity with biometrics such as face surveillance technology or with third-party data brokers; these methods are also ripe for further misuse by government entities and private companies. Moreover, neither AB 751 nor the pilot program the bill would make permanent are necessary to ensure people can safely get certified copies of vital records during the COVID-19 pandemic. People can still request vital records online by submitting a scan of a notarized affidavit of their identity. With mobile notaries and socially distanced notarization, the notarized affidavit of identity remains a safe and viable option for everyone. Straying from this proven, reliable method for identity verification threatens increased harm, identity theft, and serious privacy intrusions for all Californians.

In recent years, there have been growing concerns about how biometric surveillance, and particularly facial recognition technology, has been deployed. Facial recognition technology is being used in our electronic devices and smart home products. However, the widespread collection of data through this technology is troubling. A recent study found that there is more than a 50 percent chance that any adult is already included in a law enforcement facial recognition database.[2] A researcher at the Center for a New American Security has described the privacy concerns with such ubiquitous and powerful technology:

> If you just walk down the street in Boston, in New York, in London, you are going to be recorded by many security cameras. Some of them [in] the possession of the local police force, most of them in possession of private companies who just have a security camera. So in society, we have really gotten used to the idea of being photographed constantly. What's new in facial recognition technology is that we're losing the anonymity that used to be associated with being recorded. So it's not just that you walk past a 7-Eleven, and the security camera notes that you're there. There's the possibility that the 7-Eleven will know that you specifically, as an individual, are there, and they know how many times you have passed by in the past few weeks. That's what's really changing in recent years is the

[2] Shannon Van Sant, S*an Francisco Approves Ban On Government's Use Of Facial Recognition Technology* (May 14, 2019) NPR, https://www.npr.org/2019/05/14/723193785/san-francisco-considers-ban-on-governments-use-of-facial-recognition-technology.

> ability to analyze this data and correlate it and draw insights from it. It really does raise a whole host of new privacy concerns.[3]

The use by private businesses has also exploded in recent years:

> Facial-recognition software, which has been in development since the 1960s and has been gaining popularity with police for more than a decade, has taken off with retailers and event spaces during the last couple of years, consultants say. It's marketed to them as an unparalleled tool for cutting down on shoplifting, and sold to the public as a security tool — helping identify would-be terrorists at sports games, for instance, or protecting consumers against identity theft by making sure that they are who they say they are. It's also almost completely unregulated.[4]

In addition to the troubling privacy concerns posed by the technology, there has been research showing that the technology frequently results in misidentification, especially with persons with darker skin tones. A recent test of the technology highlighted accuracy concerns when matched with federal lawmakers:

> The errors emerged as part of a larger test in which the [ACLU] used Amazon's facial software to compare the photos of all federal lawmakers against a database of 25,000 publicly available mug shots. In the test, the Amazon technology incorrectly matched 28 members of Congress with people who had been arrested, amounting to a 5 percent error rate among legislators.
>
> The test disproportionally misidentified African-American and Latino members of Congress as the people in mug shots.[5]

A similar test was conducted with members of the California Legislature, resulting in 1 in 5 legislators being erroneously matched to a person who had been arrested when their pictures were screened against a database of 25,000 publicly available booking photos.[6]

Indeed, at both the state and local level, jurisdictions have been concerned enough to place a halt or institute outright bans on its use. AB X4 1 (Evans, Ch. 1, Stats. 2009)

---

[3] Peter O'Dowd, *As Facial Recognition Technology Booms, So Do Privacy Concerns* (Dec. 21, 2018) WBUR, https://www.wbur.org/hereandnow/2018/12/21/facial-recognition-privacy-concerns.
[4] Nick Tabor, *Smile! The Secretive Business of Facial-Recognition Software in Retail Stores* (Oct. 20, 2018) New York Magazine, http://nymag.com/intelligencer/2018/10/retailers-are-using-facial-recognition-technology-too.html.
[5] Natasha Singer, *Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says* (Jul. 26, 2018) New York Times, https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html.
[6] Anita Chabria, *Facial recognition software mistook 1 in 5 California lawmakers for criminals, says ACLU* (August 13, 2019) Los Angeles Times, https://www.latimes.com/california/story/2019-08-12/facial-recognition-software-mistook-1-in-5-california-lawmakers-for-criminals-says-aclu.

explicitly required legislative approval before the Department of Motor Vehicles could purchase or use facial recognition software. More recently, AB 1215 (Ting, Ch. 579, Stats. 2019) prohibits a law enforcement agency or law enforcement officer from installing, activating, or using any biometric surveillance system in connection with an officer camera or data collected by an officer camera, until January 1, 2023.

In just the last two years, multiple California cities have also banned its use. San Francisco has banned its use by police and government agencies.[7] Oakland followed suit, and according to the Oakland City Council President, "the ban was instituted on the basis that facial recognition is often inaccurate, lacks established ethical standards, is invasive in nature, and has a high potential for government abuse."[8] Alameda also banned the use of such systems in 2019, asserting "its potential abuse could undermine civil liberties and the technology was unreliable."[9] Berkeley's city council banned its use by its police department and other public agencies.[10]

Despite this movement, a New York Times exposé revealed that a company specializing in the technology, Clearview AI, has aggregated over three billion images scraped from publically accessible media, including Facebook, YouTube, and Venmo, to create a database of online identities matched with images of those individuals that can be used for facial recognition.[11] Clearview AI has allegedly provided this service to over 600 law enforcement agencies, allowing identification of virtually any individual in an image so long as that individual maintains an online presence.

In fact, a lawsuit against Clearview AI was recently filed by two immigrants' rights groups in California, Mijente and NorCal Resist, to stop the company's surveillance technology from proliferating in the state.[12] The complaint alleges that the company's software is still used by state and federal law enforcement to identify individuals despite the various official bans. The suit alleges Clearview AI's database of images violates the privacy rights of people in California broadly and that the company's "mass surveillance technology disproportionately harms immigrants and communities of

---

[7] Sarah Emerson, *San Francisco Bans Facial Recognition Use by Police and the Government* (May 14, 2019) Vice, https://www.vice.com/en/article/wjvxxb/san-francisco-bans-facial-recognition-use-by-police-and-the-government.
[8] Caroline Haskins, *Oakland Becomes Third U.S. City to Ban Facial Recognition* (July 17, 2019) Vice, https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.
[9] Peter Hegarty, *East Bay police used facial recognition technology despite ban* (April 9, 2021) East Bay Times, https://www.eastbaytimes.com/2021/04/09/east-bay-police-used-facial-recognition-technology-despite-ban/.
[10] Levi Sumagaysay, *Berkeley bans facial recognition* (October, 16, 2019) The Mercury News, https://www.mercurynews.com/2019/10/16/berkeley-bans-facial-recognition/.
[11] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It* (January 18, 2020) The New York Times, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[12] Rachel Metz, *Clearview AI sued in California by immigrant rights groups, activists* (March 9, 2021) CNN, https://www.cnn.com/2021/03/09/tech/clearview-ai-mijente-lawsuit/index.html.

color." Given the permissive nature of the bill, a company like Clearview AI could be contracted with to provide the verification called for by the statute using their facial recognition technology.

Even the author agrees that "the technology is not developed enough to adequately or consistently identify individuals." The author additionally acknowledges that the sponsors of the bill, the County Recorders Association of California, "note that none of their remote identity proofing vendors use any form of biometrics, including facial recognition, for the particular reason that biometric data is not widely available for comparison purposes, nor are there collection methods developed for wide-scale commercial use." In fact, NIST itself has published data on facial recognition software and noted its inability to reliably identify individuals of various racial and ethnic groups.[13]

As opposition points out, "AB 751 would be the first explicit authorization in statute for the use of face surveillance technology by a state entity." Opening the door to the use of this technology by public officials that are issuing vital records is arguably a step in the wrong direction. The Committee may wish to consider prohibiting the use of biometric verification methods to protect Californians. If biometric verification methods overcome these challenges in the future, the Legislature can revisit the issue. The author has agreed to place a three-year moratorium on the use of biometric identification.

Amendment

Insert: "Notwithstanding clause (III) the verification pursuant to this clause shall not occur through biometric comparison. This subclause shall remain in effect only until January 1, 2025, and as of that date is inoperative."

In addition, there are some concerns with continuing to authorize the use of private entities for verification. Opposition argues:

> AB 751 also infringes on Californians' privacy rights and expectations by authorizing the use of data brokers to verify a person's identity. By sanctioning identity verification through credit reporting agencies and similar databases, AB 751 will allow third-party data companies to profit off the personal data of Californians. Some data brokers, such as Acxiom and Intelius, collect personal details about consumers' behavior online, their income, and addresses, which are used to create a detailed profile about them. This information is then sold and resold, and often used for marketing and potentially for other purposes, including lending decisions.

[13] Patrick Grother, *Face Recognition Vendor Test (FRVT)Part 3: Demographic Effects* (December 2019) NIST, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

The Committee may also wish to consider whether this verification method should be authorized indefinitely, to be used by the various public officials throughout the state.

SUPPORT

County Recorders Association of California (sponsor)
County Health Executives Association of California
Orange County Board of Supervisors
Los Angeles County Board of Supervisors
TechCA
TechNet

OPPOSITION

ACLU California Action
Consumer Federation of America
Consumer Federation of California
Electronic Frontier Foundation
Media Alliance
Oakland Privacy
Privacy Rights Clearinghouse
Secure Justice

RELATED LEGISLATION

Pending Legislation: None known.

Prior Legislation:

AB 2376 (Flora, 2020) would have deleted the sunset date in Section 103526. The bill was not heard in the Senate Judiciary Committee.

AB 1215 (Ting, Ch. 579, Stats. 2019) *See* Comment 4.

AB 2636 (Linder, Ch. 527, Stats. 2016) *See* Comment 3.

AB 464 (Daly, Ch. 78, Stats. 2013) *See* Comment 3.

AB 130 (Jeffries, Ch. 412, Stats. 2009) *See* Comment 2.

AB X4 1 (Evans, Ch. 1, Stats. 2009) *See* Comment 4.

AB 247 (Speier, Ch. 914, Stats. 2002) *See* Comment 2.

AB 1614 (Speier, Ch. 712, Stats. 2002) *See* Comment 2.

PRIOR VOTES:

Assembly Floor (Ayes 75, Noes 0)
Assembly Appropriations Committee (Ayes 16, Noes 0)
Assembly Health Committee (Ayes 15, Noes 0)

****