Date of Hearing: April 22, 2021

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 1503 (Santiago) – As Amended March 25, 2021

SUBJECT: Digital driver's licenses and identification cards

SUMMARY: This bill would authorize the Department of Motor Vehicles (DMV) to conduct a pilot program for the authorization of digital driver's licenses (DL) and identification cards (ID). Specifically, **this bill would**:

1) Permit, but not require, DMV to conduct a pilot program for the authorization of mobile or digital DL or ID cards, subject to all of the following requirements:

    - The alternative licenses must be approved by the California Highway Patrol (CHP).

    - The pilot program shall be limited to no more than 0.5% of the licensed drivers for the purposes of the evaluation.

    - The alternative products evaluated must be provided at no cost to the State.

    - The participants in the program participate in a voluntary fashion.

2) Require the pilot program to be completed by January 1, 2028.

3) Limit the data exchanged between DMV and the provider of any electronic device to the data necessary to display the information necessary for a DL or ID.

4) Authorize the pilot program to include REAL ID cards upon authorization of the United States Secretary of Homeland Security.

5) Require DMV to submit a report to the Legislature on the pilot program by July 1, 2026 that evaluates the following:

    - The cost effectiveness of the alternatives used in the pilot program.

    - An evaluation of the alternative device and if the product is able to retain information relating to the movement or location, and if so, what security features are in place to protect against unauthorized access to information.

    - Recommendations for subsequent actions, if any, that should be taken with regard to alternatives evaluated in the pilot program.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched an the persons or things to be seized." (U.S. Const., Fourth Amend.)

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

3) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. CalECPA also generally specifies the only conditions under which a government entity may access electronic device information by means of physical interaction or electronic communication with the device, such as pursuant to a search warrant, wiretap order, consent of the owner of the device, or emergency situations, as specified. (Pen. Code Sec. 1546 et seq.)

4) Establishes the Information Practices Act of 1977 (IPA), which declares that the right to privacy is a personal and fundamental right and that all individuals have a right of privacy in information pertaining to them, and generally regulates the handling of personal information (PI) by state agencies. (Civ. Code Sec. 1798, et seq.)

5) Requires, state agencies when providing by contract for the operation or maintenance of records containing PI to accomplish an agency function, to apply the requirements of the IPA to those records. (Civ. Code Sec. 1798.19.)

6) Defines, for the purposes of the IPA, PI to mean any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual. (Civ. Code Sec. 1798.3.)

7) Establishes, within the Government Operations Agency, the Department of Technology (CDT), and generally tasks the department with the approval and oversight of information technology (IT) projects, and with improving the governance and implementation of IT by standardizing reporting relationships, roles, and responsibilities for setting IT priorities. (Gov. Code Sec. 11545, et seq.)

8) Finds that the unique aspects of IT goods and services and their importance to state programs warrant a separate body of governing statutes that should enable the timely acquisition of IT goods and services to meet the state's needs in the most value effective manner. (Pub. Con. Code Sec. 12100(a).)

9) Provides that all contracts for the acquisition of IT goods and services related to IT projects, as defined, shall be made by or under the supervision of CDT as provided, and endows CDT with the final authority for all of the following: the acquisition of IT goods and services related to IT projects; the determination of IT procurement policy; the determination of IT procurement procedures applicable to IT acquisitions and telecommunications procurements; and the determination of procurement policy in telecommunications procurements. (Pub. Con. Code Sec. 12100(b)-(e).)

10) Establishes the California Consumer Privacy Act of 2018 (CCPA) and provides various rights to consumers pursuant to the Act. Subject to various general exemptions, a consumer has, among other things:

- the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI;
- the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;
- the right to access the specific pieces of information a business has collected about the consumer;
- the right to delete information that a business has collected from the consumer; and,
- the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and,
- the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

11) Establishes the California Privacy Rights Act of 2020 (CPRA), which amends the California Consumer Privacy Act of 2018 (CCPA) and creates the California Privacy Protection Agency (CPPA), which is charged with implementing these privacy laws, promulgating regulations, and carrying out enforcement actions. (Civ. Code Sec. 798.100 et seq.; Proposition 24 (2020).)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of this bill**: By authorizing the DMV to establish a pilot program to evaluate the use of digital IDs, this bill seeks to give California residents the option of carrying an official California driver's license or ID by way of an application on their phone. This bill is author sponsored.

2) **Author's statement**: According to the author:

> Currently, California law only allows for the use of physical driver's licenses (DL) or identification cards (ID). Physical DLs and IDs are often lost or stolen, leaving the individual without a proper form of identification while they wait for a replacement card, which can take up several weeks to be issued by the Department of Motor Vehicles (DMV). Without an acceptable backup, if a DL or an ID is left at home, lost or stolen, people are unable to show proof of identify. Additionally, if a licensed driver is pulled over for a traffic infraction and does not physically have their DL with them, they may face a fine. This fine could be avoided with digital DLs and DLs, as people almost always have their cell phones with them.

AB 1503 would require the DMV, by January 1, 2024, to implement the use of digital DLs and IDs to supplement existing physical forms of identification. The digitalized DL and ID would be made available for any Californian who has been granted a DL or ID by the DMV, regardless of legal status. The bill also allows the DMV to issue digital Real IDs upon authorization of the United States Secretary of Homeland Security.

Digital DLs and IDs would be accessed on a secure mobile application, in which an ID holder's personal information would be encrypted. Digital DLs and IDs would not replace a physical ID, but would be a secondary identification option.

3) **An increasingly digital world**: In 2015, Iowa became the first state to authorize a pilot program for digital DL and IDs. The following year Louisiana became the first state to authorize the use of digital DLs and IDs. Regarding Louisiana's authorization of digital DLs and IDs, Governing reported:

> Seventy-seven percent of American adults already own a smartphone, including 94 percent of adults under 30, and many state motor vehicle officials think residents will appreciate the convenience of having their driver's license available in an app.
>
> Officials also like that the licenses are connected to a central database and can be updated easily with, for example, suspensions or revocations.
>
> And unlike plastic cards that can easily be counterfeited or tampered with, mobile licenses are less susceptible to fraud, they say.
>
> But as is often the case when something analog goes digital, privacy advocates worry about the potential for government overreach and fear the digital licenses and motor vehicle databases will become vulnerable to hackers.
>
> "These are shiny new things, and states are only talking about the upsides," said Chad Marlow, a senior counsel at the American Civil Liberties Union in New York. "It is very important the public understand there are significant risks with digital driver's licenses. I think it is irresponsible for states to offer them without explaining those risks." […]
>
> To address privacy concerns, the [Louisana] law says that displaying a digital license doesn't serve as consent or authorization for police or anyone else to search or view any other data or app on the mobile device.[…]
>
> But critics such as the ACLU's Marlow are skeptical that digital licenses in Louisiana or anywhere else are a good idea.
>
> By unlocking the license, phone owners could expose their data to whoever is checking it, Marlow said. And, he added, while an officer normally would need a warrant to search a phone, in the real world, drivers who don't know the law could be pressured into handing over the phone, allowing access to everything from contacts to text messages.

> And he worries hackers could access data being transmitted to and from the DMV database.[1]

To date, a total of 11 states have either authorized or are currently conducting a pilot program authorizing the use of digital DLs or IDs. In December of 2020, the REAL ID Act of 2005 was explicitly amended to authorize the use of digital DL and ID cards.

In 2015, Governor Brown vetoed AB 221(Dababneh), which would have required DMV to study the feasibility of implementing a digital DL. In his veto message, the Governor wrote, "while the idea of a digital license sounds innovative, it poses numerous technical difficulties. Given the many new responsibilities that the Department of Motor Vehicles is already dealing with, I don't believe this bill is advisable."

To get around the challenges posed by AB 221, this bill would authorize a private company to develop a pilot program, so long as it is at no cost to the state, similar to the pilot authorized by SB 806 (Hueso, Ch. 569, Stats. 2013), which authorized DMV to establish a pilot program to evaluate the use of alternatives to license plates, registration stickers, and registration cards.

4) **The bill in print would create a pilot program for digital DL and ID cards, but lacks some critical privacy and security protections**: As it is currently in print, AB 1503 would authorize DMV to establish a pilot program to evaluate the use of mobile or digital alternatives to DL and ID cards, and would require any such pilot program to conform to certain specifications. Those specifications include: (1) receiving approval from CHP for the alternative licenses; (2) limiting participation in the pilot to no more than 0.5% of licensed drivers; (3) ensuring any pilot is carried out at no cost to the state; (4) requiring the pilot to be completed by January 1, 2028; (5) limiting any data exchanged between DMV and any electronic device or the provider of any electronic device pursuant to the pilot to only what is necessary to display the information necessary for the DL or ID; and (5) limiting participation to only those who volunteer to do so. 0

   The bill would also authorize DMV to evaluate the inclusion of participants in the Business Partner Automation Program in the conduct of any such pilot, and would, subject to authorization by the United States Secretary of Homeland Security, permit the issuance of mobile or digital "Real ID" DLs and IDs. Finally, the bill would require DMV, should it conduct such a pilot program, to submit a report to the Legislature no later than July 1, 2026 that includes: (1) an evaluation of the cost-effectiveness of the alternatives used in the pilot compared to current IDs and DLs; (2) a review of all products evaluated in the pilot and features of those products, including if the devices are available with the ability to transmit and retain information relating to the movement and location, and, if so, whether the product includes security features to protect against unauthorized access to that information; and (3) recommendations for subsequent actions that should be taken with regard to the alternatives evaluated.

   The provisions of the bill in print outline a general framework for a pilot program to test digital IDs and DLs, but relies largely on the discretion of DMV, and of any contracting entity, to implement the pilot in a manner that is sufficiently considerate of privacy and

---

[1] Bergal, *States Weigh the Benefits and Challenges of Digital Driver's Licenses*, (Nov. 21, 2018) Governing.

security. Notably, the bill in print entertains the possibility of implementing digital IDs and DLs with the capacity to collect and retain highly sensitive PI such as geolocation information, and seemingly considers "any security features to protect against unauthorized access to information" as optional, even if such sensitive information is collected. Additionally, the bill in print, like many state programs, appears to establish cost as the preeminent consideration, requiring any pilot be conducted at no cost to the state and that the report include an evaluation of cost-effectiveness of alternatives tested and compared to physical IDs and DLs.

While immediate cost is inevitably a factor in the conduct of all state programs, arguably, the privacy and security of the PI of program participants should supersede cost. The information contained on a DL or ID is fundamentally identifying, and, if compromised, could easily facilitate identity theft. Furthermore, because mobile applications can, either intentionally or through malicious modifications, access sensitive information such as location information, personal conversations, and even health and financial information stored on the phone, security considerations for any such program should be paramount. Staff notes that such security concerns materialized earlier this year, when a security breach at a DMV contractor potentially compromised the PI of tens of millions of Californians.[2] Should the data security of pilot participants, or of any successor emerging from the pilot, be compromised, the State may face costly liability due to negligence should security not be proactively prioritized. Because the stakes of failure to protect privacy and security in this instance are so substantial, a post hoc assessment of those characteristics in the report to the Legislature is arguably insufficient, and the explicit provision of privacy and security protections seems essential.

To ensure that any pilot program established pursuant to AB 1503 would provide suitable privacy and security protections, the author has offered several amendments that would significantly strengthen the bill. These amendments would:

- Provide that a participate in any pilot program established by the department pursuant to the bill may terminate their participation in the pilot at any time, and may, upon termination, request the deletion of any data associated with their participation in the program; and require that DMV and all entities contracted with DMV for the purpose of effectuating the pilot delete all data collected or maintained pursuant to the participants participation in the pilot within 10 days of the request.

- Explicitly require that, in developing and implementing the use of digital DLs and IDs, DMV ensure the protection of PI and include security features that protect against unauthorized access to information, including, but not limited to: (a) ensuring that the digital DL or ID, as well as any mobile application required for the digital DL or ID, shall not contain or collect any information not strictly necessary for the functioning of the digital DL, ID, or mobile application, including but not limited to location information; and (b) ensuring that the information transmitted to the digital DL or ID, as well as any mobile application required for the digital DL or ID, is encrypted and

[2] Joshua Bote, "California DMV hit by data breach, exposing millions of drivers' personal information to hackers," *SFGate*, Feb. 18, 2021, https://www.sfgate.com/bayarea/article/California-DMV-hit-data-breach-ransomware-attack-15959944.php, [as of Apr. 20, 2021].

protected to the highest reasonable security standards broadly available and cannot be intercepted while being transmitted from DMV.

- Prohibiting an entity contracted with DMV for the purpose of the pilot from using, sharing, selling, or disclosing any information obtained as part of the contract, including, but not limited to any information about the holder of a digital DL or ID, except as necessary to satisfy the terms of the contract; and requiring that, upon termination or expiration of the contract, the contracting entity delete any data collected or generated in the course of activities pursuant to the contract within 30 days.

- Clarify that any data exchanged between DMV and any electronic device, between DMV and the provider of any electronic device, and between any electronic device and the provider of that device, shall be limited to those necessary to display the information necessary for a DL or ID.

- Strike the assessment of cost-effectiveness from the required report to encourage prioritization of security and privacy considerations.

5) **Fourth Amendment considerations**: The Fourth Amendment states, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const. 4th Amend.) Stated another way, it prohibits Government from intruding on a person's right of privacy in their own person, home, papers, and effects, unless the Government first obtains a warrant issued upon probable cause supported by sworn testimony and stating the place to be searched and the persons or things to be taken possession of. A warrant thus demonstrates that the search and seizure is "reasonable" as required by the Fourth Amendment's prohibition against "unreasonable searches and seizures."

   While much of the early Fourth Amendment search doctrine focused on whether the Government "obtains information by physically intruding on a constitutionally protected area," more recent judicial precedent recognizes that "property rights are not the sole measure of Fourth Amendment protections." (*See Carpenter v. United States* (2018) 138 S.Ct. 2206, 2213, citing (*U.S. v. Jones* (2012) 565 U.S. 400 and *Soldal v. Cook County* (1992) 506 U.S. 56.) In the seminal case of *Katz v. United States* 389 U.S. 347, 351 the U.S. Supreme Court established that "the Fourth Amendment protects people, not places." In doing so, the Court "expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' [the Supreme Court] has held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." (*Carpenter,* 128 S.Ct. at 2213.)

   Though Fourth Amendment jurisprudence concerning mobile devices is still nascent, it has generally been established that modern cell phones generate a greater expectation of privacy than other personal effects. For instance, in *People v. Sandee* (2017) 15 Cal. App. 5th 294, the court explained:

> Following the United States Supreme Court's opinion in *Riley v. California* [citation], it is firmly established that a law enforcement officer may not conduct a search of a person's cell phone without a warrant, even incident to arrest, unless an applicable exception to the warrant requirement applies. As *Riley* observed, "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be carried on an arrestee's person." [Citation] *Riley* explained that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life,' [citation]. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." (*Id.* at p.300.)

Despite this unique consideration, one notable exception to "the warrant requirement" is consent. If a person freely and voluntarily consents to the search, the Fourth Amendment right against warrantless searches is effectively waived, even if the person is not aware of their right to refuse.

One circumstance in which DLs and IDs are commonly used for identity verification is in encounters with law enforcement. In, for example, a traffic stop, the DL is generally handed to the officer, who uses it to record certain information, and then hands it back to the driver. However, in the case of a digital DL carried on the person's mobile device, "freely and voluntarily" handing the device to the officer, unlocked so as to provide access to the digital DL, specifically for the purpose of the officer extracting certain information, could potentially be construed as consenting to a search of the device. Even if the officer is only intending to view the information on the DL, mobile devices often display incidental information, such as incoming text messages or calls, and other notifications, with the potential to incriminate the participant. Additionally, since digital DLs and IDs provide the possibility for remote assessment of the DL or ID, a person may give consent for such remote access by law enforcement, which could be interpreted as consent to access the device as a whole. Given the abundance and sensitivity of PI available on a person's mobile device, this categorical difference from the practical use of a physical DL therefore arguably warrants specific provisions to ensure participants in a digital DL and ID pilot do not unwittingly waive their Fourth Amendment rights. Accordingly, the author has offered several amendments that would directly address circumstances in which Fourth Amendment rights could be implicated in a digital ID and DL pilot program. Specifically, these amendments would:

- Require that, in developing and implementing the use of digital DLs and IDs, DMV ensure the protection of PI and include security features that protect against unauthorized access to information, including, but not limited to: (a) ensuring that use of the digital DL or ID does not require handing over one's digital device to any other person or entity; and (b) ensuring that any remote access to the digital DL or ID shall require the express, affirmative, real-time consent of the person whose digital DL or ID is being requested for each piece of information being requested, and shall be limited to only that information which is provided on a physical DL or ID card.

- Specify that the holder of a digital DL or ID card shall not be required to turn over their electronic device to any other person or entity in order to use it for identity verification.

- Provide that the holder of a digital DL or ID card showing or turning over their electronic device to any other person or entity to use it for identity verification shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital DL or ID; and further provide that information incidentally obtained in the process of viewing a digital DL or ID in order to verify the identity of the holder shall not be used to establish probable cause for a warrant to search the device.

- Require that any request for remote access to the digital DL or ID for identity verification require the express consent of the holder of the digital DL or ID, be limited to the content of the digital DL or ID specified in the request for remote access, and not exceed the information available on a physical DL or ID.

- Provide that consent to remote access to a digital DL or ID by the holder shall not constitute consent to a search, nor shall it constitute consent for access to any information other than that which is immediately available on the digital DL or ID; and further provide that information incidentally obtained in the process of remotely accessing a digital DL or ID shall not be used to establish probable cause for a warrant to search the device.

6) **Other considerations addressed by author's amendments**: In addition to several technical and clarifying amendments, the author has also offered amendments to expand on the voluntary nature of the program and address potential equity concerns that could arise from a program that requires an often costly personal device in order to access a critical government document. To clarify that any pilot program would be strictly voluntary in all respects, the author has offered amendments that would:

   - Specify that DMV would be authorized to establish a pilot program to evaluate the use of *optional* mobile or digital alternatives to DLs and IDs.

   - Require that all participants receive both a physical and digital DL or ID.

   - Provide that a participant in a pilot program shall not be required to use a digital DL or ID rather than a physical DL or ID for the purpose of identity verification, nor shall their participation in the pilot program preclude their use of a physical DL or ID under any circumstances.

   - To ensure that any pilot program established pursuant to the bill would be equitably administered, the author has offered amendments that would:

   - Require that alternative products evaluated pursuant to a pilot program be provided at no cost to the participant.

   - Prohibit a person or entity from providing preferential service based on a person's use of a digital DL or ID rather than a physical DL or ID.

7) **Related legislation**: AB 984 (Luz Rivas) would make permanent the pilot program for alternative license plates and registration cards.

8) **Prior legislation**: SB 806 (Hueso, Ch. 569, Stat. 2013) authorized DMV to establish a pilot program to evaluate the use of alternatives to license plates, registration stickers, and registration cards.

   AB 221(Dababneh, 2015) would have required DMV to study the feasibility of implementing a digital DL. That bill was vetoed by Governor Brown.

9) **Double referral**: This bill was double referred to the Assembly Transportation Committee where it was heard on April 5, 2021 and passed 13-0.

REGISTERED SUPPORT / OPPOSITION:

Support

None on file

Opposition

None on file

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