
THIRD READING

Bill No: AB 2769
Author: Cooper (D), et al.
Amended: 6/28/18 in Senate
Vote: 21

SENATE GOVERNMENTAL ORG. COMMITTEE: 9-1, 6/12/18
AYES: Dodd, Wilk, Cannella, Gaines, Galgiani, Glazer, Hill, Hueso, Portantino
NOES: Vidak
NO VOTE RECORDED: Bradford, Lara

SENATE JUDICIARY COMMITTEE: 5-2, 6/26/18
AYES: Jackson, Hertzberg, Monning, Stern, Wieckowski
NOES: Moorlach, Anderson

SENATE APPROPRIATIONS COMMITTEE: 5-2, 8/16/18
AYES: Portantino, Beall, Bradford, Hill, Wiener
NOES: Bates, Nielsen

ASSEMBLY FLOOR: 73-0, 5/17/18 (Consent) - See last page for vote

SUBJECT: Privacy: driver's license information

SOURCE: Author

DIGEST: This bill authorizes businesses to scan driver's licenses and identification cards for the same purposes and under the same limitations that current law allows for the swiping of such documents.

ANALYSIS:

Existing law:

- 1) Provides that a business may swipe a driver's license or identification card issued by the Department of Motor Vehicles (DMV) in any electronic device for the following purposes:

- To verify age or the authenticity of the driver's license or identification card;
 - To comply with a legal requirement to record, retain, or transmit that information;
 - To transmit information to a check service company for the purpose of approving negotiable instruments, electronic funds transfers, or similar methods of payments, provided that only the name and identification number from the license or the card may be used or retained by the check service company; or
 - To collect or disclose personal information that is required for reporting, investigating, or preventing fraud, abuse, or material misrepresentation. (Civ. Code Sec. 1798.90.1(a)(1).)
- 2) Provides that an organ procurement organization may swipe a driver's license or identification card issued by the DMV in any electronic device to transmit information to the Donate Life California Organ and Tissue Donor Registry for the purposes of allowing an individual to identify as a registered organ donor. Information gathered or transmitted pursuant to this paragraph shall comply with the DMV Information Security Agreement. Before swiping, the organization must provide clear and conspicuous notice to the applicant and shall follow specified procedures. (Civ. Code Sec. 1798.90.1(a)(2).)
- 3) Prohibits a business or organ procurement organization from retaining or using any information obtained by these electronic means for any purpose other than as provided. (Civ. Code Sec. 1798.90.1(a)(3).)
- 4) Provides that a violation of the above provisions constitutes a misdemeanor punishable by imprisonment in a county jail for no more than one year, or by a fine of no more than \$10,000, or by both. (Civ. Code Sec. 1798.90.1(c).)

This bill allows the scanning of driver's licenses and identification cards for the same purposes as they may currently swipe such identification documents, and subjects the scanning of these documents to the same restrictions as current law imposes on the swiping of the documents.

Background

Current law allows businesses to swipe driver's licenses and identification cards issued by the DMV for extremely limited purposes, such as to verify the age of the holder or the authenticity of the card. However, businesses are explicitly prohibited from retaining or using the information gained through the swiping of the cards for any purpose other than those provided. Violations of these provisions can subject persons to misdemeanor charges and a fine of up to \$10,000.

Recent technology has allowed for the *scanning* of driver's licenses by businesses to perform these same functions. However, there is evidence that businesses selling or using this technology are not following the guidelines laid out in existing law that regulate the swiping of licenses and identification cards. In fact, businesses are not only collecting personal information from the scanning of these cards but are also retaining the data, analyzing it, and sharing it with other businesses.

This bill authorizes the scanning of driver's licenses and identification cards to the same extent as current law allows the swiping of such identification documents.

Comments

The author writes:

AB 2769 updates existing privacy law to account for new technology and protect people's personal information and right to privacy.

Since 2003, it has been illegal for any entity that "swipes" a person driver's license or identification card when verifying a person's age or authenticity of their ID to collect, retain or share any data, except to assist in a criminal investigation. AB 2769 updates current law to include when an entity "scans" [a] person's ID.

AB 2769 seeks to protect everyone's personal data. This bill does not ban scanning technology, it allows for businesses to use this technology and protects an individual's right to privacy by ensuring that this technology, that is becoming an industry standard is well-regulated, as it should be.

Addressing the widespread collection and sharing of consumers' personal information

SB 602 (Figueroa, Chapter 533, Statutes of 2003) established the Identity Theft Prevention and Assistance Act to prevent and punish identity theft. Included therein are provisions that prohibit businesses from "swiping" the magnetic strips on driver's licenses except for limited purposes, such as to verify age or authenticate the license. Such businesses are prohibited from retaining or further using the encoded information, except where otherwise authorized by law. (Civ. Code Sec. 1798.90.1.) The Senate Judiciary Committee's analysis of the bill indicates that these provisions "stem from recent press reports that some businesses, such as bars and clubs, have been retaining information from licenses swiped to verify age. According to the press accounts, in some instances this information has been used to market to individuals who have had their license read

in this way.” The statute was later amended to authorize swiping of licenses for organ donation purposes.

All data transferred to or from the DMV or other third party servers is encrypted utilizing the most up-to-date protocols to maintain the privacy and confidentiality of data while it is transported over the Internet. These security controls and compliance steps were enacted to protect the confidentiality, integrity, and availability of DMV information and the information systems authorized to process, store, and transmit that information.

This bill amends the statute to now allow for new scanning technology. Just as with SB 602, this bill was motivated by recent news stories describing the practice of some bars scanning driver’s licenses and identification cards and the concerns that this data was being retained by the businesses scanning them. The author states the belief that this “practice of keeping persons’ personal data from the electronic scan of a person’s ID should already be illegal under state law.”

The widespread collection of personal information of consumers without clear regulation raises serious privacy concerns. Current law clearly prohibits the retention of information collected through the *swiping* of licenses and identification cards. However, there is a lack of clear law preventing the retention of the same data when those cards are *scanned*. This bill amends the above statute and equates scanning with swiping, closing this gap.

Existing scanning practices are problematic

Concerns about scanning technology being used to systematically collect and share personal information are not just theoretical. PatronScan is a scanning company that has established its own network in California and beyond. In a letter of opposition to a previous version of this bill, it admitted that it had collected and *retained* information from 561,087 customers. This statistic is limited to the first five months of 2018 and only includes Sacramento. The population of the City of Sacramento recently topped 500,000 people for the first time.

PatronScan’s director of sales and marketing was interviewed in the article cited as motivation by the author. In it, he admits that all the information is retained for at least 90 days. It can also be kept longer if the *company* determines there is a “public safety need” or the consumer is placed on a “banned” list. The company admits that it not only retains this information but flags the entries with additional information that it then shares with other businesses regulated by the Department of Alcoholic Beverage Control.

Documents shared by PatronScan show that the information is not simply being kept for security reasons. A “Public Safety Report” from the company provides a snapshot of a single day of scans comprising over 10,000 unique customer scans. The data in the report collects information about where the customers live, how far they have travelled, and how many different venues the customers patronized. It also shows how serious its banning function can impact a customer, indicating that the average ban was over 19 years.

Probably farthest from its reported security function, the report lays out the demographics, average household size, and average household income of the various locations the customers are coming from. Such widespread collection of data without any clear indication customers are being told such information is being collected, retained, and analyzed is of questionable legality under current law.

The security concerns around the collection of such information were highlighted in another report regarding the breach of Target’s information systems. It raised questions concerning whether Target’s practice of collecting data from driver’s licenses could have also been compromised. If these scanning networks collect vast information about consumers, including tags connecting them to where they have been, the dangers from breaches are concerning.

Additional concerns arise from the ability of this information to be shared with federal immigration officers. Scans of driver’s licenses and identification cards, especially those authorized pursuant to AB 60 (Alejo, Chapter 524, Statutes of 2013), could lead to problematic practices in the industry.

The restrictions imposed by this bill on scanning address these privacy concerns.

FISCAL EFFECT: Appropriation: No Fiscal Com.: Yes Local: Yes

According to the Senate Appropriations Committee, potential local assistance costs, not likely to be significant.

SUPPORT: (Verified 8/17/18)

None received

OPPOSITION: (Verified 8/17/18)

City of Sacramento
Downtown Sacramento Partnership

Midtown Association
PatronScan

ARGUMENTS IN OPPOSITION: PatronScan writes in opposition, “In striking the balance between privacy protections and patron safety, PatronScan would like to maintain the ability to share *limited* information from scans conducted at ABC-licensed entities specifically with other businesses licensed by ABC for the sole purpose of providing information to those licensees to grant or deny entry into their establishments based on safety considerations.”

ASSEMBLY FLOOR: 73-0, 5/17/18

AYES: Acosta, Aguiar-Curry, Travis Allen, Arambula, Baker, Berman, Bigelow, Bloom, Bonta, Brough, Burke, Caballero, Calderon, Carrillo, Cervantes, Chau, Chávez, Chen, Chiu, Choi, Chu, Cooley, Cooper, Cunningham, Dahle, Daly, Eggman, Flora, Fong, Frazier, Friedman, Gallagher, Eduardo Garcia, Gipson, Gloria, Gonzalez Fletcher, Gray, Grayson, Harper, Holden, Irwin, Jones-Sawyer, Kalra, Kamlager-Dove, Kiley, Lackey, Levine, Limón, Low, Maienschein, Mathis, Mayes, McCarty, Medina, Mullin, Nazarian, Obernolte, O'Donnell, Patterson, Quirk, Quirk-Silva, Reyes, Rodriguez, Rubio, Salas, Mark Stone, Thurmond, Ting, Voepel, Waldron, Weber, Wood, Rendon

NO VOTE RECORDED: Cristina Garcia, Melendez, Muratsuchi, Santiago, Steinorth

Prepared by: Christian Kurpiewski / JUD. / (916) 651-4113
8/18/18 13:41:56

**** END ****