



May 8, 2017

Senate Transportation and Housing Committee
State Capitol, Room 2209
Sacramento, CA 95814
Phone: (916) 651-4121
Fax: (916) 445-2209

Re: S.B. 712 and California's Constitutional Right to Privacy

Dear Chairperson Beall and members of the Committee,

Over the last few days, multiple aides for Committee members requested that EFF provide further information in writing on S.B. 712 and the privacy principles enshrined in the California Constitution.

As we explained in our previous letter, the Electronic Frontier Foundation is a member-supported non-profit organization based in San Francisco that protects civil liberties at the intersection of technology in the law. Founded in 1990, EFF has over 36,000 members around the world, including thousands in California. We are proud to serve as sponsors for this legislation.

The California Constitution, Article 1, Section 1 establishes that pursuing and obtaining privacy is an “inalienable right.”¹ The successful 1972 constitutional amendment was specifically designed to protect Californians from computerized, mass surveillance. The proponents of the amendment (California State Assemblymember Kenneth Cory and California State Senator George Moscone) told voters the following in their ballot argument:

The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create

¹ California Department of Justice. “Privacy Laws.” Online: <https://oag.ca.gov/privacy/privacy-laws>

“cradle-to-grave” profiles of every American.

At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian.

The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose. It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.²

In the 1975 case *White v. Davis*, the California Supreme Court applied the California constitutional right to privacy in a case in which Los Angeles police officers were gathering intelligence on university students without any suspicion of criminal activities. The court held that “the routine stationing of covert, undercover police agents in university classrooms and association meetings, both public and private, constitutes ‘government snooping’ in the extreme.”³

Similarly, automated license plate readers (ALPRs) collect billions of sensitive data points on American drivers with the overwhelming majority of data collected absent any suspicion of a crime. In fact, some law enforcement officials argue that they want this data just in case a driver eventually, one day, potentially years in the future, commits a crime.

In its letter opposing S.B. 712, the League of California Cities told this committee that “individual privacy concerns should not trump public safety.” This wrongheaded position runs counter to the constitutional duties of government officials across California.

² Argument in Favor of Proposition 11, at http://repository.uchastings.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.

³ *White v. Davis*, 13 Cal. 3d 757, 775-76 (1975).

The cost of ALPR isn't just tax dollars, but also our privacy: law enforcement is subsidizing companies that turn our privacy into a commodity to be sold to some of the most abusive and discriminatory industries. For example, using ALPR data, lenders screen our travel patterns before approving a loan; insurance companies inspect our travel patterns before providing a quote; and debt collectors and repossession companies use the data to track targets down.

To argue the public safety value of ALPRs, law enforcement has provided marketing materials from a particular company, Vigilant Solutions. All of the examples in the press releases were three years old and none occurred in California, and the anecdotes are unclear as to whether they involved moving or stationary vehicles. In addition, one should be skeptical that law enforcement agencies will provide this committee with balanced information. Contracts between agencies and Vigilant Solutions often include non-disparagement and non-publication clauses that stymie the ability for the public to receive honest assessments of ALPR technology. For example, the clauses below were included in a City of Lodi contract with Vigilant Solutions in 2016:

(d) Non-Publication. Agency shall not create, publish, distribute, or permit any written, electronically transmitted or other form of publicity material that makes reference to the LEARN Software Service or this Agreement without first submitting the material to Vigilant and receiving written consent from Vigilant thereto. This restriction is specifically intended to ensure consistency with other media messaging.

(e) Non-Disparagement. Agency agrees not to use proprietary materials or information in any manner that is disparaging, This prohibition is specifically intended to preclude Agency from cooperating or otherwise agreeing to allow photographs or screenshots to be taken by any member of the media without the express consent of Vigilant. Agency also agrees not to voluntarily provide ANY information, including interviews, related to Vigilant, its products or its services to any member of the media

without the express written consent of Vigilant.⁴

In addition to violating the Constitution right to privacy, this contract with Vigilant Solutions further violates Section 3(b)(1) of the California Constitution, which establishes “the right of access to information concerning the conduct of the people’s business ... and the writings of public officials and agencies shall be open to public scrutiny.” The contract also runs counter the California Public Records Act, which states “access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person in this state.”

We conclude this letter in the same way the California Supreme Court concluded its *White v. Davis* opinion—with a prescient quote from 19th century English historian, Sir Thomas Erskine May:

Next in importance to personal freedom is immunity from suspicions and jealous observation. Men may be without restraints upon their liberty; they may pass to and fro at pleasure: but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators,—who shall say that they are free?

ALPRs are nothing short of a contemporary version of the surveillance state that the authors of the 1972 amendment, the California Supreme Court, and Sir May warned about. In 2017, our “steps” are our driving patterns and the “spies and informers” are high-speed cameras that upload our location data to a massive, searchable database.

S.B. 712 would work towards fulfilling our right to pursue and obtain privacy by allowing drivers to block their plates from ALPRs when lawfully parked. This is a balanced approach, since S.B. 712 would not affect law enforcement’s ability to collect ALPR data from moving vehicles.

A vote against S.B. 712 is to agree that the state may tie our hands and allow private companies and law enforcement to record our comings and goings en masse and to use this information against us without any suspicion of criminal activity.

⁴ Vigilant Solutions Enterprise Service Agreement. Online: <https://www.documentcloud.org/documents/3520531-Lodi-2016-6.html>

Please do not hesitate to contact me with further questions regarding S.B. 712. I may be reached by email at dm@eff.org or by phone at 415-436-9333 ext. 151.

Sincerely,

A handwritten signature in black ink, appearing to read "DMAS", is centered on the page. The signature is written in a cursive, somewhat stylized font.

Dave Maass
Investigative Researcher
Electronic Frontier Foundation