ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

May 3, 2017

Senator Joel Anderson
State Capitol, Room 5052
Sacramento, CA 95814
Phone: 916.651.4038
Fax: 916.651.4938

Re: S.B. 712 – SUPPORT AS AMENDED MAY 1, 2017

Dear Senator Anderson,

On behalf of the Electronic Frontier Foundation (EFF - Sponsor), I write today to express our support for S.B. 712, a bill that would enhance Californians' privacy by adjusting the current vehicle code to allow drivers to attach a removable cover to their license plates when lawfully parked.

EFF 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 collection of location data by automated license plate readers (ALPRs) by private companies represents what The Atlantic has described as an "unprecedented threat to privacy."[1] ALPR systems are high-speed cameras that capture the plate numbers of any vehicle that passes within view. ALPRs convert the images into machine-readable data, tag the data with a time stamp and global position, and upload the information to a central database. Often these systems are pre-loaded with "hot lists," or lists of vehicles identified for special scrutiny; the camera systems alert users when these vehicles are captured by an ALPR.

Private companies have amassed billions of plate scans, which they store indefinitely. These companies market this data to law enforcement agencies

[1] Friedersdorf, Conor. The Atlantic. "An Unprecedened Threat to Privacy." January 27, 2016. Online: https://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/

815 Eddy Street • San Francisco, CA 94109 USA
voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

and private companies, particularly those involved in the financial industry. Companies offer advanced analytical tools that promise to predict a vehicle's travel patterns or identify associates through vehicles often spotted in the vicinity. Users may even plug in a particular location to identify vehicles that have visited or passed nearby.

These cameras represent a grave threat to our individual liberties as well as public safety. Currently, nothing prohibits ALPR companies from making this data more widely available. One security breach could result in sensitive location data being leaked online. In addition, these databases are ripe for abuse by individuals with access or who share their access with others.

This data puts a wide variety of individuals at risk. The data could be used to stalk domestic violence victims. It could be used to surveil religious centers, law firms, medical centers, gun shows, and protests. This data could be used by political campaigns to monitor their opponents.

In addition, this data puts law enforcement at great risk: if exposed, this data could reveal information about the home lives of law enforcement officials and judges as well as information about ongoing investigations.

These threats will only increase in severity with the advancement of technology. A private company may soon deploy autonomous vehicles affixed with ALPRs in order to comprehensively collect sensitive location information from an entire city, almost like data-scraping Roombas for the streets. Car sharing services may one day augment their fleets with ALPRs in order to increase their profit margins. As the technology becomes more publicly accessible, criminal enterprise could collect data from a city the size of Oakland with only two vehicles in less than a week.[2]

Current law prohibits individuals from augmenting their license plates to avoid ALPRs, with one important exception: a driver may cover their entire vehicle when lawfully parked to protect their vehicle from the elements. It stands to reason that if a person may cover their entire car, they should be allowed to cover just their plate as well. This is common sense.

---

[2] Gillula, Jeremy and Dave Maass. EFF Deeplinks. "What You Can Learn from Oakland's Raw ALPR Data." Online: https://www.eff.org/deeplinks/2015/01/what-we-learned-oakland-raw-alpr-data

This bill would not affect the ability of law enforcement to collect ALPR data from moving vehicles. Officers would also be authorized to inspect a lawfully parked vehicle's plate beneath a plate cover.

The impact of this bill would be to allow individuals to protect their privacy when they are engaged in sensitive though lawful activity. When parked at home or when visiting a location that they would like to keep confidential (such as visiting a doctor) they could cover their plate to protect it from being captured by ALPRs.

This legislation would also address an economic unfairness. Apple pioneer Steve Jobs famously purchased new cars on a regular basis in order to avoid having a static license plate.[3] Wealthier drivers are able to afford homes with closed garages or overnight parking, while drivers with fewer resources must park with their license plates exposed in their driveways or on the street.

This bill presents a balanced solution. It does not put further mandates on law enforcement. It does not present a burden for private companies. Instead, it allows members of the public a way to defend their privacy from invasive data-gathering processes.

EFF commends you for bringing this legislation. Please do not hesitate to contact me to discuss how we may further lend our assistance to passing S.B 712. I may be reached by email at dm@eff.org or by phone at 415-436-9333 ext. 151.

Sincerely,

Dave Maass
Investigative Researcher
Electronic Frontier Foundation

[3] The legislature has addressed this issue, but it does not take affect until 2019. Gitlin, Jonathan. Ars Technica. "California closes the Steve Jobs license plate loophole." Online: https://arstechnica.com/cars/2016/07/steve-jobs-loophole-closed-california-wants-temporary-license-plates/