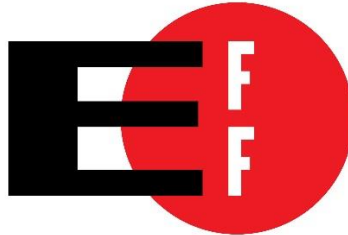




Calegislation

consumer action
Education and advocacy since 1971



April 15, 2015

The Honorable Ben Hueso
State Capitol, Room 4035
Sacramento, CA 95814

Re: SB 249 (Hueso) – Oppose as introduced

Dear Senator Hueso:

The American Civil Liberties Union of California, Calegislation, Consumer Action, Consumer Watchdog, Eagle Forum of California, Electronic Frontier Foundation, Gun Owners of California, and Privacy Rights Clearinghouse regret to inform you of our opposition to SB 249. This measure would allow the DMV to issue “Enhanced Drivers Licenses” (EDLs) to U.S. citizens who could use them at the Canadian and Mexico land borders as proof of citizenship. We have profound privacy and security concerns about the use of insecure Radio Frequency Identity (RFID) computer chips in EDL identity documents.

1. The use of long-range Radio Frequency Identification (RFID) chips raises concerns about privacy, safety and the creation of fraudulent identity documents.

SB 249 authorizes the California Department of Motor Vehicles to enter into a memorandum of understanding with a federal agency to begin issuing EDLs that have a unique identifying number – which is personal information under California law¹– embedded in a long-range RFID computer chip. As the Cato Institute has noted about the personal identification number, “Think of it as your Department of Homeland Security Tracking number.”²

¹ California Civil Code 1798.3 defines “personal information” as “any information that identifies or describes an individual, ...”

² Jim Harper, *Do Not Walk, California – Run from EDLs*, Cato at Liberty, August 16, 2013
<http://www.cato.org/blog/do-not-walk-california-run-edls>

The Department of Homeland Security (DHS) has admitted that the personal identification information encoded on the RFID chip could be read from up to 30 feet away. There are no technological protections included on the RFID chip, or in the EDL document itself, to keep this personal information from being read without an individual's knowledge or consent. Devices have already been built that can read and clone the RFID tag on an EDL.³ As currently designed, there is nothing to stop someone from building similar readers to make counterfeit EDLs that could be used as a border-crossing document, engage in identity theft, or improperly track and monitor the activities of innocent Californians.

The American Electronics Association (AeA), the Smart Card Alliance (an industry trade group), and leading electronics companies have warned the US Department of State and the Department of Homeland Security that long-range, insecure RFID technology is not appropriate for the EDL:

- “highly susceptible to forgery.” (AeA)
- “A potential illicit hacker could very easily read (again from a distance) the unique ID contained . . . and easily create a duplicate.” (AeA)
- “Perversely maximize the possibility . . . of an illicit actor ‘tracking’ a person at very long ranges . . . would potentially threaten individual U.S. Citizen privacy.” (AeA).
- Basic RFID technology does not have the necessary technological protections to eliminate the risk of terrorists, criminals, or illegal aliens . . . spoofing or counterfeiting PASS cards to enter the United States undetected.” (Smart Card Alliance)

Significant privacy and security concerns were also expressed by Congress and the Department of Homeland Security's own Data Privacy & Integrity Advisory Committee who cautioned against the use of RFID technology for identifying people.⁴ The DHS Inspector General noted, in reviewing the Customs and Border Patrol's traveler programs, that “[a]dditional security controls [such as encryption] would be required if CBP . . . migrates to universally readable” RFID chips, such as those proposed to be used in the EDL.⁵

Contrary to the contentions asserted in the bill about the benefits of the EDL, testing by the United States government “raised numerous issues about the reliability and performance of the RFID technology.”⁶

³ *EPC RFID Tags in Security applications: Passport Cards, Enhanced Drivers Licenses and Beyond*. Profs. Koscher, Juels, Brajkovic, Kohno. available at <http://homes.cs.washington.edu/~yoshi/papers/RFID/ccs280-koscher.pdf>

⁴ *Security and Privacy Issues Associated With Federal RFID-Enabled Documents*. Center for Democracy and Technology (July 2008). <https://cdt.org/insight/security-and-privacy-issues-associated-with-federal-rfid-enabled-documents/>

The Use of RFID for Human Identification. A Report of the DHS Data Privacy & Integrity Advisory Committee http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

⁵ *CBP's Trusted Traveler Systems Using RFID Technology Require Enhanced Security*: A Report of the Office of the DHS Inspector General available at http://www.oig.dhs.gov/assets/Mgmt/OIGr-06-36_May06.pdf

⁶ *Border Security: US-Visit Program Faces Strategic, Operational, and Technological Challenges at Land Use Ports of Entry*. Report of the Government Accountability Office available at <http://www.gao.gov/new.items/d07248.pdf>

2. EDL Lacks Basic Security Deployed in U.S. e-Passports.

Despite the likelihood that Californians would be carrying an EDL in their wallets daily and potentially using it many times a day for identification purposes under this bill, the EDL as currently proposed does not even have the basic security and privacy features that are found in the U.S. e-passports, as shown in the table below.

Passport	EDL
Random identification number generated each time RFID is read	Same unique identification number used each time RFID tag is read
Data embedded in the RFID is encrypted (scrambled so it cannot be read by an eavesdropping RFID reader)	Identification number transmitted without encryption (can be read by an eavesdropping RFID reader)
Passport cover contains metal threads to block RFID data transmission when the passport is completely closed (Note: protection fails when passport is open greater than ¼ of an inch)	EDL do not have built-in shielding security. (If a protective sleeve is distributed with the new cards, Californians must understand the importance of using the sleeve and remember to do so. Personal information (the personal identification number) is vulnerable when the card is removed from the sleeve.
Intended read-range of RFID tag is 2-3 feet.	RFID tag expected to transmit up to 30 feet.

3. SB 249 Includes No Enforceable Safeguards for Californians' Privacy & Security

The United States government requires a “take it or leave it” approach to EDLs in order to ensure that all systems and cards are compatible in any state that adopts an EDL. States are prohibited from including additional technical privacy and security measures like encryption or authentication that would make them more secure.⁷ This means that the language in the bill, “...that shall be encrypted if agreed to by the United States Department of Homeland Security...”⁸ is illusory. Thus, if EDLs are allowed to move forward, the personal information of Californians will be very vulnerable.

While EDLs are proposed to be optional now and the bill includes some language to deter employers from requiring use of the EDLs, optional government electronic programs often turn into permanent mandatory programs. For example, optional electronic toll lanes on the Golden Gate Bridge have now disappeared and you must use electronic tolling to cross the bridge.⁹

⁷ “If, in the future, the States collectively determine that it is feasible to introduce encryption, DHS may consider such an effort so long as the encryption program enables law enforcement easy access to the information in the MRZ.” Preamble to the final regulations p, 86, 144) quoted in CDT Testimony to Senate Committee on Homeland Security and Governmental Affairs (2008) available at <https://cdt.org/files/testimony/20080429scope-written.pdf>

⁸ See 15401(d)(1)

⁹ <http://goldengate.org/tolls/faqs.php>

4. SB 249 Would Undermine Driver's License Information Privacy.

California law (Cal. Civ. Code 1798.90.1) safeguards the confidentiality of driver's license information by allowing businesses to swipe the magnetic strip on the back of the licenses and use or retain the information only for limited purposes, such as age verification and fraud prevention. Because a magnetic strip cannot be read at a distance, Californians know when their information is being read by others and can take action to enforce the law and protect their privacy.

If the DMV issues EDLs with long-range, insecure RFID technology, any person, business, or agency with a compatible reader could potentially acquire a Californian's EDL number (similar to an electronic social security number or "Department of Homeland Security tracking number") and build up a database without the affected people ever knowing about it. The California constitutional right to privacy was intended to protect people from the type of unknown collection of information that is facilitated by insecure RFID technology.

5. California Should Not Move Forward With Insecure EDLs

It has long been understood that the federal government selected the most insecure RFID technology for WHTI-compliant documents like the EDL without a proper assessment of costs and benefits or attention to the significant and well-supported privacy and security concerns expressed by lawmakers, the electronics industry, security researchers, the public, and its own internal experts. California should not make the same mistake.

We must therefore strongly oppose SB 249.

Sincerely,



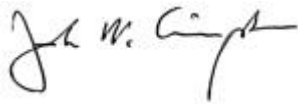
Kevin G. Baker
Legislative Director
American Civil Liberties Union of California

Dian Black

Dian Black
Legislation Director
Calegislation

Joe Ridout


Joe Ridout
California Legislative Director
Consumer Action



John M. Simpson
Privacy Project Director
Consumer Watchdog

Orlean Koehle

Orlean Koehle
State President
Eagle Forum of California



Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation



Sam Paredes
Executive Director
Gun Owners of California



Beth Givens
Executive Director
Privacy Rights Clearinghouse

cc: Members and committee staff, Senate Judiciary Committee