Why the Enhanced Driver's License is Wrong for California

What is an Enhanced Driver's License?

The Enhanced Driver's License (EDL) is a new government identification document being promoted by the Department of Homeland Security to satisfy the mandate of the Western Hemisphere Travel Initiative (WHTI).

WHTI, passed by Congress in 2004, requires that anyone crossing the land borders of Canada and Mexico after January 31, 2008, present a passport, a federal PASS Card or another approved citizenship document in the form of an "enhanced" driver's license.

Significant Privacy and Security Problems- EDL Not Appropriate for California

- DHS is currently proposing that the California DMV issue EDLs that have personally identifiable information, in the form of a unique identifying number, encoded on a long-range RFID computer chip.

- DHS has admitted that the personal 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 the personal information from being read without an individual's knowledge or consent.

- Security researchers have already built devices that can read and clone the RFID tag on an EDL. [1] As currently designed, there is nothing to stop someone from building similar readers to make counterfeit enhanced drivers' licenses, engage in identify theft, or improperly track and monitor the activities of innocent Californians.

AeA, Smart Card Alliance, and leading electronics companies warned the US Department of State and the Department of Homeland Security in January 2006 that long-range, insecure RFID technology was 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)

[1] See *EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond* available at http://www.rsa.com/rsalabs/node.asp?id=3557

- "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 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)

EDL Lacks Basic Security Deployed in US e-Passports

While it is likely that Californians would be carrying an EDL in their wallet on a daily basis and potentially using it many times a day for identification purposes, the EDL as currently proposed does not even have the basic security and privacy features that are built into the US e-passports.

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 tag is encrypted (scrambled so it can not 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 passport is completely closed. (Note: protection fails when passport is open >1/4 inch)	EDL does not have built-in shielding security. Although protective shield sleeves will be distributed with new cards, Californians must understand the importance of placing the EDL in the sleeve and remember to do so. Personal information is also vulnerable every moment the EDL is removed from the shield for use.
Intended read-range of RFID tag is 2-3 feet.	RFID tag expected to transmit up to 30 feet.

EDL Would Eviscerate Driver's License Information Privacy

California law, Cal. Civ. Code 1798.90.1, safeguards the confidentiality of driver's license information by only allowing businesses to swipe the magnetic strip on the back of the license and use or retain the information 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, organization, or company with a compatible reader could attempt to read and record a Californian's EDL number and build up a database of information about individuals without an individual ever knowing that the information has been read. Such a scenario would be wholly incompatible with the California Constitution, which guarantees a right to privacy, and was intended to protect individuals from exactly the type of unknown collection of digital information that is facilitated by insecure RFID technology.