Enhanced Drivers' Licenses With Insecure RFID Technology: Setting the Record Straight

Myth: The EDL is secure.
Fact: The unencrypted personal information on the RFID chip in an EDL can be read at a distance of 30 feet without an individual ever knowing that it has been read or who has read it. If EDLs are deployed in California, the personal information of Californians could be stolen without a trace.

Fact: Insecure RFID technology has been cracked many times, all over the world.

- Leading security researchers built a device for $250 in spare parts, drove around San Francisco, and read and copied the travel documents of people walking down the street without them ever knowing (2009)
- Cracked the Sacramento Capitol identification cards and gained access to member-only, secure entrances (2006)
- Cracked the RFID chips used in the Dutch and British e-passport (2006)
- Cracked the RFID chips in the Exxon Mobil gasoline-payment passes & in car anti-theft devices (2005)

Leading electronics organizations and companies warned the US Department of State and the Department of Homeland Security that long-range, insecure RFID technology was not appropriate for use in the Enhanced Driver's License.

- "highly susceptible to forgery." "A potential illicit hacker could very easily read (again, from a distance) the unique ID contained…and easily create a duplicate." "Perversely maximize the possibility…of an illicit actor 'tracking' a person at very long ranges…would potentially threaten individual U.S. citizen privacy." (American Electronics Association)
- 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)

The Department of Homeland Security's own Data Privacy & Integrity Advisory Committee also cautioned against the use of RFID technology and the DHS Inspector General noted that additional security measures like encryption would be needed if they wanted to move forward with this type of technology.

Myth: The EDL does not transmit any personal information, just a number.
Fact: The EDL will transmit personal information under California law.
Each enhanced drivers' licenses will be encoded with a unique identifying number –it's like a DHS social security number- and unique identifying numbers like this are personal information under California law.[1]

Myth: SB 249 provides for encryption of EDLs in California.
Fact: The U.S. government requires a "take it or leave it" approach to EDLs and it is currently prohibited for states to include additional technical privacy and security measures like encryption or authentication that would make them more secure. SB 249 bill also fails to include any provisions requiring shielding or other physical tamper-resistant measures, basic protections that can and should be added to any use of EDL and have been found to effectively reduce the potential of long-range unknown reading and other tampering.

Myth: EDLs only be read at border crossings.
Fact: EDLs can be read anywhere, by anyone with a reader (including building one with $250 in spare parts), from up to 30 feet away, without anyone ever knowing, since an EDL has no encryption or other security measures.

---

[1] California Civil Code 1798.3 defines "personal information" as "any information that identifies or describes an individual, including, but not limited to…social security number…"