Mother Jones

California Votes on Driver's Licenses That Allow the Government (and Anyone With $40) to Stalk You

The enhanced IDs contain a chip that can be read via radio 50 meters away.

By Dana Liebelson | Wed Aug. 21, 2013 3:00 AM PDT

California's Assembly Appropriations Committee is expected to vote on a bill Wednesday that would give residents the option of getting a "driver license on steroids [1]." The enhanced IDs, which are recommended by the Department of Homeland Security (DHS), act as an international E-ZPass—complete with a microchip holding a unique ID number that can be read via radio up to 50 meters away [2]—and can be used to drive across borders between Canada and Mexico.

Drivers who have them don't have to bring their passports and can move through border checkpoints more quickly. (They can also be used in the Caribbean, although the drive-through feature doesn't apply.) But privacy advocates say that there's a dangerous catch: Unlike with passports, which are encrypted, anyone with a simple Radio Frequency Identification (RFID) scanner—like this one available for $37.95 on Amazon [3]—can read the unique number broadcasted by these new IDs, determine if the card's owner is nearby, or even replicate the number to steal the owner's identity.

Additionally, that ID number can be used (by someone with access to the Department of Homeland Security database) to pull up a secure DHS file containing, at minimum [4], "biographical information, a photo, and the results of terrorist/criminal checks." The bill doesn't provide any caps on whether other information, like that collected by the National Security Agency, can be included in the database as well. Michigan, New York, Vermont, and Washington already offer these insecure IDs—but civil liberties advocates say that the more states that adopt this technology, the more likely it is that they will eventually become mandatory.

"An individual that does not understand the privacy and security risks of an Enhanced Driver's License (EDL) might think, 'Why not get an one so that I can use it to drive and also cross the border?' It seems like common sense," says Nicole Ozer, technology and civil liberties policy director at the ACLU of California. "But the cost to privacy and security far outweighs any benefits. If you carry one of these licenses in your wallet or purse, you can be tracked and stalked without your knowledge or consent."

The RFID chips work by emitting a unique identification number—not that different from a social security number—to readers that operate on a certain radio frequency. This is somewhat similar to the chips embedded in passports [5], except that passports generate random identification numbers each time they're read, only broadcast information a few feet, and are encrypted [6]. None of that is true with federally approved enhanced IDs, nor with PASS Cards, according a comprehensive study [2]done by the University of Washington in 2009. (But PASS Cards, which act as alternatives to passports for North American travel, aren't as likely to be carried by Americans on a day-to-day basis.) US Customs and Border Protection [7] claims that "no personal information is stored or transmitted" from an enhanced ID—but the unique ID number that is transmitted is used to

"point to the information housed in the secure database," which can include names and photos. DHS did not respond to questions posed by *Mother Jones* about what else is included in the database.

Senate Bill 397 [8], which was introduced by Democratic state Sen. Ben Hueso, aims to bring California's ID standards up to those of DHS's Western Hemisphere Travel Initiative [9], which in 2007 required visitors from the United States, Canada, Mexico, and Bermuda to have a passport, PASS Card, or an enhanced driver's license to cross borders. "Sen. Hueso authored this bill to reduce border wait times and increase economic gain produced by efficient and secure cross-border travel," says Lourdes Jimenez, a spokesperson for his office. "This is strictly an optional program." However, Jim Harper, director of information policy studies at the Cato Institute, notes that "introducing enhanced IDs as optional is part of the glide-path toward adoption. It allows the kinks to be worked out and a baseline group of users to be created, so it's less difficult to make mandatory in the future."

Jimenez notes that "[a]ll information embedded in the RFID chip is encrypted and securely transmitted, via a unique reference number, from the card to the Customs and Border Protection network." However, these RFID chips must meet a federal standard set by DHS, and in 2006 [10], DHS's own privacy committee found that "the use of RFID-enabled systems could ultimately aid the monitoring of individuals' movements (tracking.)" The privacy committee also found that RFIDs "merely identify the credential, not the individual bearing it," because the ID cards did not have the encryption to prevent cloning.

Senate Bill 397, in its current form, also does not say that only border control agents are permitted to scan enhanced IDs and access the DHS database—the same right could potentially be extended to local law enforcement. (DHS did not comment on who is permitted to access the database.) "So if I'm the police—to use an extreme example—I can gather the movements of everyone

holding an EDL by putting scanners in airports, hotels, street corners, and everyplace else," says Cato's Harper. "Then when I want to find out where everyone has been, I just link my data to the DHS data."

Jimenez says that "the number on its own has no meaning until an authorized reader transmits it to a secure government database." However, Ozer argues that even without access to a DHS database, anyone with an Amazon-purchased RFID scanner could, at minimum, determine where someone is going and replicate their unique ID number. In 2006, she says, the ACLU successfully cloned the RFID chips on the identification held by a California lawmaker—and was able to get into the state capitol through an authorized entrance. "At the very least, the author of this bill should not allow the police to use it to surreptitiously track Californians and include a proper shield device to help ensure that the licenses cannot be read without someone's knowledge or consent," she says. "We have urged the author to take this amendment and so far, he has refused."

Hueso's office says that it has worked with ACLU on other amendments, such as "inserting language in the bill that requires the DMV to inform all EDL applicants, either orally or in writing, that the randomly assigned number can be read remotely without the holder’s knowledge." Jimenez also says the bill requires "reasonable security measures," such as protective sleeves be used—but right now, the sleeves that are issued under federal regulations don't stop the cards from being read, according to the University of Washington study. Several materials, including water, metal, and Mylar, do prevent RFID tags from being read. Alternatively, here's what happens when you put the RFID chip in the microwave [11].