American Civil Liberties Union
(ACLU) of Arizona
PO Box 17148
Phoenix, AZ 85011
www.acluaz.org

For more information contact:
Alessandra Soler Meetze
ACLU-AZ Executive Director
Tel: 602-650-1854
Fax: 602-650-1376

Enhanced Drivers' Licenses and Real ID

- **Enhanced Driver's License and Real ID are two separate programs**.
  The Enhanced Driver's License (EDL) and Real ID are based on two different Congressional mandates with divergent requirements.
  - EDL is an attempt to satisfy the mandate of the Western Hemisphere Travel Initiative, which was passed by Congress in 2004, and requires that anyone crossing the land borders of Canada and Mexico after January 31, 2008 present a passport or similar documentation of citizenship.
  - Real ID was passed in 2005, attached to a military spending and tsunami relief bill. It requires that states adhere to national standards in issuing driver's licenses, share driver records with each other and the federal government, and bars individuals who do not have a Real ID-compliant license from boarding an airplane (even for domestic travel), enter a federal building, and any other purpose designated by the Secretary of Homeland Security.

- **The Department of Homeland Security is hitching Real ID to EDL in a last-ditch effort to save it.**

  States have balked at the massive cost – over $23 billion – and the invasion of privacy represented by Real ID, and many have called into question whether the program will ever actually be implemented. The Department of Homeland Security (DHS) has repeatedly delayed implementation and has failed to issue final regulations for compliance.

  Because border states are also concerned about maintaining cross-border commerce, DHS has used the upgrade to EDL as a way to lure states into agreeing to comply with Real ID.

  This attempt to leverage EDL as a tactic to secure cooperation with Real ID is a mistake for the following reasons:

  - **Real ID is a failed program**. Citing costs, and privacy concerns, seven states (GA, ME, MT, NH, OK, SC, and WA) have passed legislation barring implementation of Real ID. Two other states (CO and ID) have passed resolutions pledging that they will not spend any money on it, and an additional eight have passed resolutions asking Congress to repeal the underlying Act. Real ID is widely acknowledged to be in deep trouble, if not doomed.

  - **If salvaged, Real ID will become America's first genuine national ID**. Real ID represents a remarkable shift away from America's traditions of liberty and personal privacy. Its requirements would make differences between state ID's merely cosmetic. Further, the physical card will be reinforced by a single, interlinked, national database containing Americans' most sensitive information such as social security numbers and birth certificates. This database will be an irresistible honey pot not only for government tracking, but also for criminal identity thieves.

  - **Signing on to Real ID before seeing final regulations is irresponsible.** DHS has failed repeatedly to issue regulations that would tell the states what they actually need to do in order to comply with Real ID. Until these final regulations are promulgated, it is anyone's guess what Real ID implementation actually means. At this point, Real ID is little more than a pig in a poke. To sign on to a program without any formal indication of what it will entail – and *how much it will cost* – is disturbingly irresponsible governance.

- **The Enhanced Driver's License has privacy problems of its own.**

  DHS's requirements for EDL include the use of Radio Frequency Identification (RFID) technology, which has proved highly insecure and has even been abandoned by DHS in other contexts. RFID chips emit a radio signal that transmits data up to 30 feet away. As such, they allow remote tracking of the license holder, by government officials or anyone else who buys an RFID reader over the internet. The data transmitted by RFID is also highly vulnerable to hacking and cloning. Shortly after the U.K. introduced RFID chips into their passport, a hacker cloned the chip, encoding an innocent person's data into a fraudulent passport.

The measures DHS is proposing to secure the RFID chip in the EDL would be laughable if they weren't so alarming: a tin foil envelope to hold your license and an "awareness" campaign. DHS claims additional protections are not needed since all the EDL will broadcast is a unique identifying number, but that's exactly what a Social Security number is – a unique identifying number that does not in itself contain private information about you, but can be used to access your most sensitive data.

DHS cannot claim to be unaware of the problems inherent in RFID technology – they abandoned its use in the US-VISIT program because of insurmountable technological hurdles. The Department's own Data Privacy and Integrity Committee warned against using RFID for tracking and monitoring of people, because of security risks of "skimming" and intercepting the signal, and the potential for broader tracking of individuals' movements and activities. EDL will do exactly what DHS's own privacy committee warned against.

- **Real ID is not needed to create a border-crossing driver's license.**
  An enhanced license for border crossing can be created without buying into the failed Real ID program. That's exactly what the state of Washington is doing. Last year, Gov. Christine Gregoire signed the first Memorandum of Agreement with DHS to create an EDL that would substitute for a passport at the border. At the same time, she signed a bill passed by the state legislature to refuse implementation of Real ID unless and until the Federal Government provides a substantial portion of the funding and builds privacy protections into the program. Neither of these conditions is likely to be met by DHS or the Congress (in fact, this summer the U.S. Senate *rejected* appropriating $300 million for Real ID implementation), so Washington has effectively opted out.

SPECIFIC PROBLEMS WITH UNIQUE IDENTIFIERS & RFID CHIPS

- ✓ While unique ID numbers make it more difficult for unauthorized readers to retrieve driver's license information (which will include a person's name, address, date of birth and social security number) it's still possible. It's basically like a key to your house, if you figure out how to access the key and unique identifier, then you'll be able to open the door.

- ✓ The world of RFID is in its early stages, and there are still tremendous security concerns. Arizona should have done its research before agreeing to implement enhanced driver's licenses.

- ✓ The most significant privacy problem with the unique identifier on an RFID chip is that it can be cloned. It's a tremendous security hole.

- ✓ The RFID chip merely spits out a unique ID that anyone who can read (using a hand-held, store bought scanner) can rewrite into a new chip. This is done by having the implanted chip also encode some (relatively) unclonable aspect of the person the chip is embedded in, e.g., you can still "steal" the unique ID, but could only then use it in a chip in another (1) female; with (2) brown eyes; (3) blood type AB-; etc.; etc.

- ✓ A completely different category of threats arises when hackers or criminals cause valid RFID tags to behave in unexpected (and generally malicious) ways. Typically, computer-bound or mobile RFID readers query RFID tags for their unique identifier or on-tag data, which often serves as a database key or launches some real-world activity. For example, when an RFID reader at a supermarket checkout counter reads the tag on a product, the software driving it could add the item scanned to the list of the customer's purchases, tallying up the total after all products have been scanned.

- ✓ Here is where the trouble comes in. Up until now, everyone working on RFID technology has tacitly assumed that the mere act of scanning an RFID tag cannot modify back-end software, and certainly not in a malicious way. Unfortunately, they are wrong. In our research, we have discovered that if certain vulnerabilities exist in the RFID software, an RFID tag can be (intentionally) infected with a virus and this virus can infect the backend database used by the RFID software. From there it can be easily spread to other RFID tags. No one thought this possible until now.

- ✓ RFID chips can still be uniquely identified by their radio behavior. Specifically, these chips have a unique identification number used for collision avoidance. It's how the chips avoid communications problems if you put a bagful of them next to a reader. This is something buried deep within the chip, and has nothing to do with the data or application on the chip. Chip manufacturers don't like to talk about collision IDs or how they work, but researchers have shown how to uniquely identify RFID chips by querying them and watching how they behave. And since these queries access a lower level of the chip than the passport application, an access-control mechanism doesn't help.