AMERICAN CIVIL LIBERTIES UNION of OHIO

TO: House Transportation & Public Safety Committee

FROM: Gary Daniels, Chief Lobbyist, ACLU of Ohio

DATE: May 17, 2017

RE: House Bill 60

To Chairman Green, Vice Chair Greenspan, Ranking Member Sheehy, and members of the House Transportation and Public Safety Committee, my name is Gary Daniels, chief lobbyist for the American Civil Liberties Union of Ohio ("ACLU of Ohio") and I appear to present opponent testimony on House Bill 60.

AMERICAN CIVIL LIBERTIES UNION OF OHIO FOUNDATION
4506 CHESTER AVENUE
CLEVELAND, OH 44103-3621
T/216.472.2220
F/216.472.2210
WWW.ACLUOHIO.ORG
contact@acluohio.org

House Bill 60 is not a complicated bill. It requires the Director of Public Safety to enter into an agreement with the Department of Homeland Security so Ohio can start producing enhanced drivers' licenses for its citizens. The stated goal of passing such legislation, in Ohio and other states, is to make crossing the Canada and Mexico borders more efficient for U.S. travelers.

However, the ramifications of HB 60 and the use of these enhanced licenses are far-reaching and fraught with privacy and security problems this committee should be fully aware of as it considers this bill.

First, the security concerns. These licenses will utilize radio frequency identification (RFID) technology to easily identify travelers. RFID is used in a variety of other ways including to track and identify everything from warehouse inventories to library books, to manage access to particular rooms, buildings, and properties, and to keep track of our pets, should they become lost.

Unfortunately, RFID chips for enhanced driver's licenses are unencrypted. This has been a concern with EDLs for years, yet their obsolete security has not improved. This is in contrast to passports, newer credit cards, and even text messages, all of which enjoy the protections of encryption.

Because these RFID chips remain unencrypted, Ohioans who use EDLs will be at risk. This is because these licenses are susceptible to forgery, cloning, and hacking without such protection.

These concerns are not exclusive to the ACLU and other advocates, as the U.S. Congress[1], the Data Privacy & Integrity Advisory Committee[2], and the DHS Inspector General[3] have all expressed similar worries.

---

[1] "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/

Indeed, in an effort to prove how easily this technology can be compromised, a security researcher drove through San Francisco in 2009, using a $250 RFID reader and an antenna, where he obtained details of two passports in twenty minutes of searching. Had he wished, he could have cloned these passports and they would have passed as actual ones.

This situation can be improved via use of a sleeve provided by DHS to be used by license holders to store and hold their cards. Of course, these sleeves offer no protection for those who do not use them or lose them. Perhaps that will be no problem for those among us who never forget anything, never misplace valuable items, and are always 100% prepared for traveling.

The ACLU of Ohio is also concerned about the ability of these licenses to be used as an eventual method to track the movements and personal information of your constituents. In 2017, it should come as no surprise that the federal government busies itself with exhausting every possible avenue to glean more data about all of us - who we call, mail, email and text, our social media posts and habits, our financial transactions, and much, much more.

If the past is any indication, it also seems that any and every technology that becomes widely used is eventually used by government for surveillance, even if that is not the original purpose for its introduction. Given the impossible-to-quench thirst of our federal government for every detail about our lives, would it be a surprise if enhanced driver's licenses were to become the latest method to keep tabs on all us?

Proponents will reply to say EDLs do not store personal information and, after all, their use is not mandatory. Given the ACLU's numerous past experiences with technology and surveillance, we think a fair reply to both those points is to say – not yet. And if the NSA, DHS, FBI and all the rest were to ignore the capabilities of EDLs to provide even more information about ourselves, we suspect it might become the very first instance where our government did not capitalize on such an opportunity.

The ACLU of Ohio has no reason to believe sponsors and supporters of this bill want to compromise personal information, compound the problems of identity and data theft, or grow our surveillance state. Nonetheless, these are the problems that arise from the use of enhanced driver's licenses. For these reasons, we urge you to reject House Bill 60.

---

[2] Report No. 2006-02 – "The Use of RFID for Human Identify Verification" - Data Privacy & Integrity Advisory Committee, Dec. 2006 - https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

[3] OIG 06-36 - "CBP's Trusted Travelers Systems Using RFID Technology Require Enhanced Security" – DHS Office of Inspector General, May 2006 – https://www.oig.dhs.gov/assets/Mgmt/OIGr-06-36_May06.pdf