

James Moyer  
james@moyer.com

### Testimony in opposition of HB 60

About me: I have twenty years experience studying identity cards, biometrics and passports, in Ohio, the United States, and globally. I have reported to this legislature, the federal government, the European Commission, and EU nations on matters related to citizen identity systems.

Key points:

- This bill has been rejected by this legislature before.
- This bill has been rejected by others, such as the North Dakota legislature.
- Security errors made in statute are difficult to fix. The best example of that is the printing of SSNs on driver's licenses, a practice approved unanimously by this legislature in 1967 and which lasted well after it was known to be a bad practice.
- The security issues of the unencrypted RFID chip found in the EDL are so bad, that the proposed statute (as well as statutes in other states) require that citizens waive liability for the RFID. **Otherwise, the identity card manufacturer would not be able to issue the product.**
- Even with the liability waiver, **the EDL is shipped with a security sleeve that the card must be kept in at all times.**
- That is an absurd state of affairs; it is an act of negligence on the part of state DMVs, DHS and the identity card manufacturer who are involved with this program.
- I wouldn't testify against this bill if it affected a small percentage of Ohioans who would opt-in for this program.
- The problem with this bill, as occurred in Washington State, is that it is likely that DHS will decide that only Ohio's EDL is REAL ID Act compliant, thereby requiring most Ohioans to participate in this program.
- 80% of Washington State ID cards now issued are EDLs due to this. For that to occur in Ohio would be a disaster.
- This is likely due to the currently legal status of Ohio's REAL ID Act compliant cards.
- This committee needs to treat this bill **as a \$25 fee increase for all Ohioans.**

- Such an outcome would mean that Ohio would have no control over its identity card program. The EDL program does not exist in federal statute, it exists only administratively. If Ohio went down the EDL path, the state identity card program would be entirely subject to the whims of DHS.
- Ohio should not be in the business of issuing international travel documents. Driver's license fraud is not improved by mixing it with passport fraud.

---

attachments:

a.) Testimony submitted to the North Dakota House Transportation Committee

*This is a highly graphical explanation of the problem with the EDL's unencrypted RFID chip. Some information in this document is now anachronous in minor detail but the document remains accurate.*

b.) May 16, 2017 letter to Rep. Hambley and Rogers' offices

*This document is a convenient list of the many problems with HB 60 and offers various solutions.*

c.) Testimony submitted to the Ohio House Transportation Committee

d.) Page 196 of Supplement 1: Contract between the State of Ohio and Veridos for Ohio driver's licenses

*The contract for the manufacture of Ohio driver's licenses is at least 500 pages. Perhaps 60-80 pages of the document resemble page 196.*

Chairman Ruby, committee members:

**Issue 1: This bill is completely unnecessary.**



=**\$65** extra, valid for **SIX** years



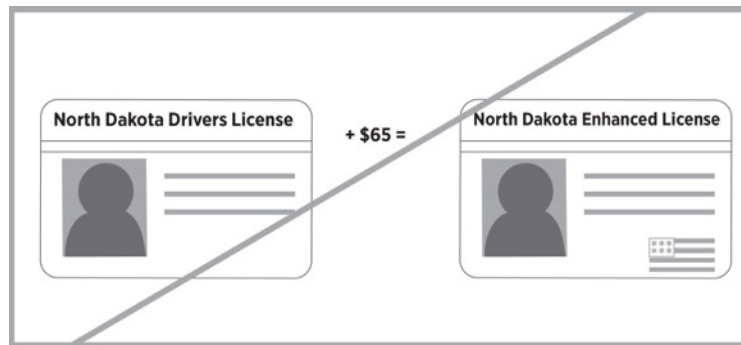
=**\$55** valid for **TEN** years.

**Questions:**

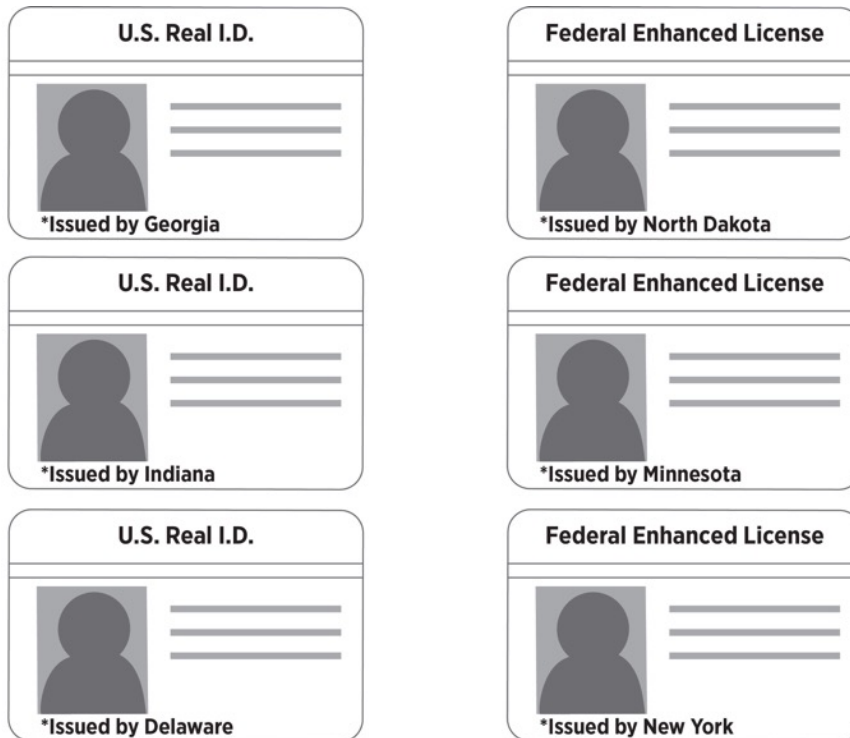
- 1.) Why would someone buy the enhanced license instead of the cheaper, longer-lasting US Passport Card?
- 2.) What problem does this card solve that isn't already solved?
- 3.) Why would the legislature be asked to create it?

## Issue 2: This is a national ID card.

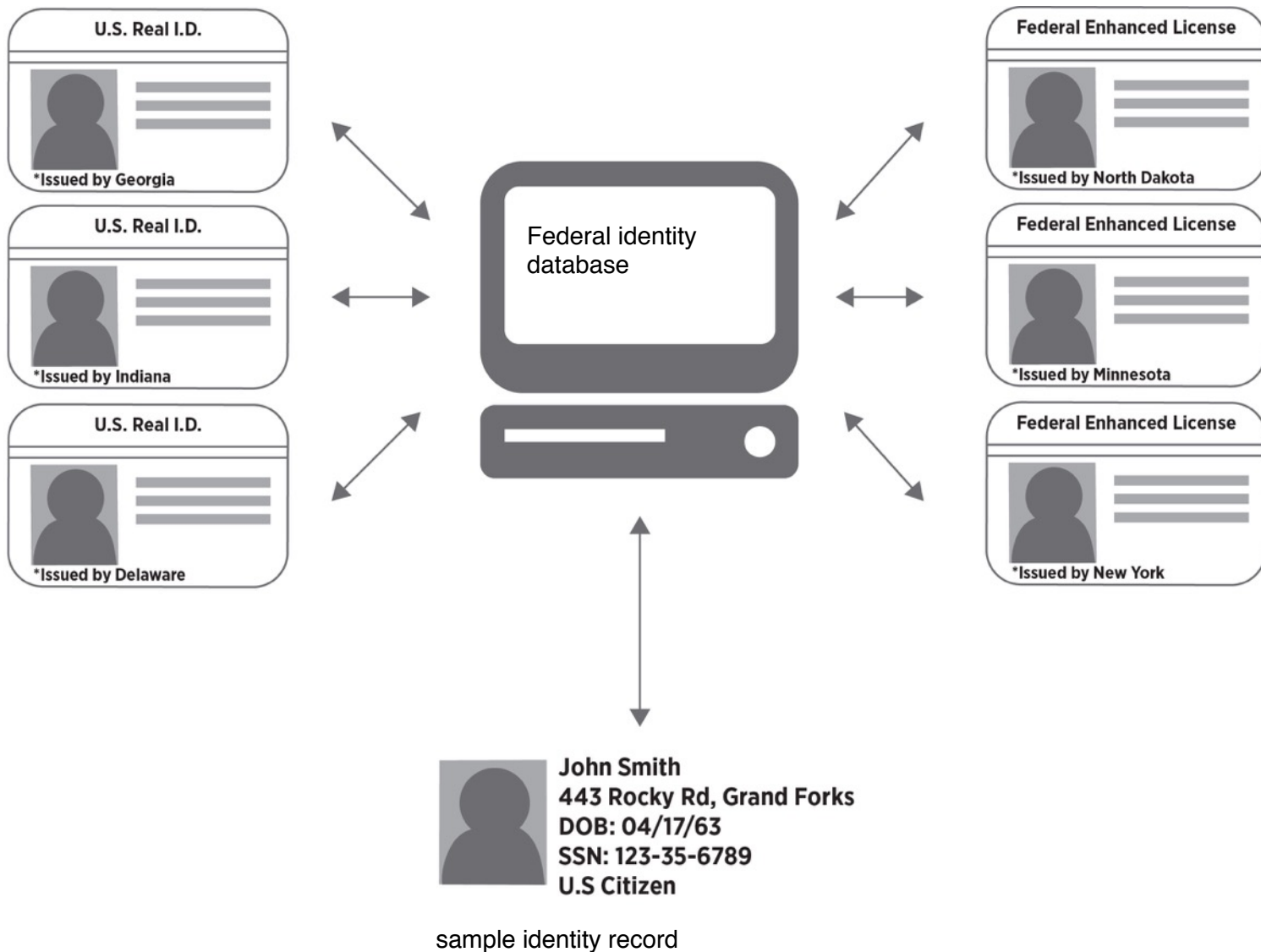
Do not make the mistake of thinking of this card is merely a North Dakota license with an additional citizenship indicator.



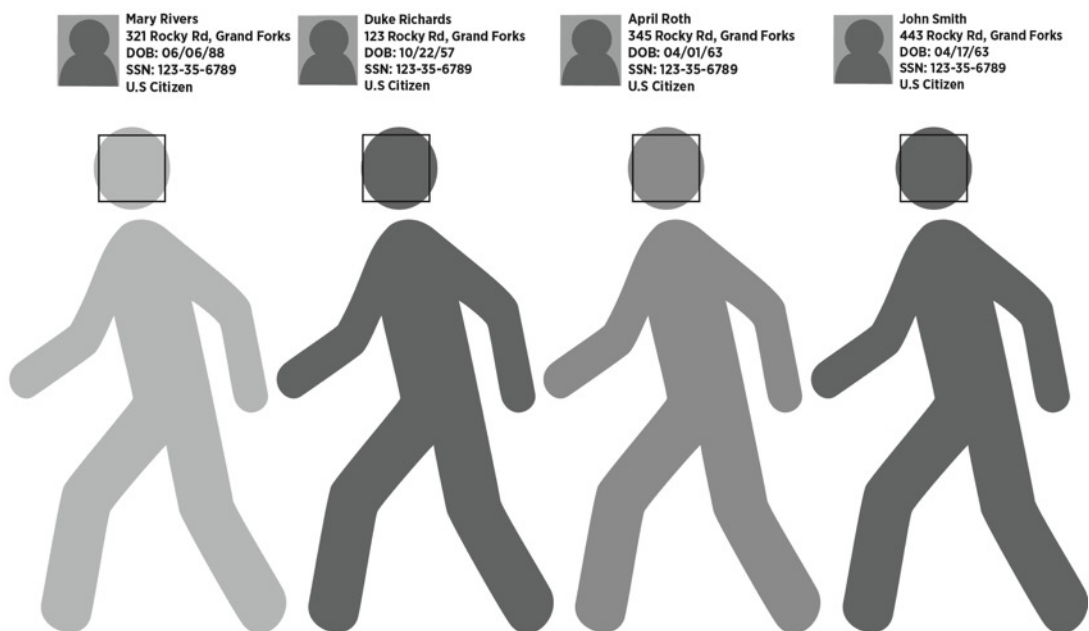
This is a federalized ID card. It's form, content, and application are determined by federal rule. ***The issuing state is merely a franchisee.*** This is also the case for the REAL ID Act.



More importantly, as a requirement for participation in the program, and like the REAL ID Act, it requires that the licensee's information found in the North Dakota identity database be accessible to the federal government.



The federalized ID card database makes it easier to fulfill surveillance state objectives, such as using facial recognition in large crowds, based on the photographs of citizens from the various states.



A camera network connected to this database would allow for easy tracking of citizens, thanks to the photograph archive and enhanced facial recognition capabilities.

At this time there are no legal barriers to the implementation of such a system.

### Issue 3: The RFID chip used in the EDL is insecure

Though the legislation says that the RFID chip “must be encrypted if agreed to by the United States department of homeland security”, DHS has not agreed with other states that have similar requirements **and all states issue enhanced licenses with unencrypted chips**. Since the chip broadcasts a unique identification number this allows for the tracking of enhanced licensee holders as shown.

Many Android phones and the iPhone 6 are able to read the RFID on the proposed enhanced license.

For a complete list of phones which will be able to read the EDL chip, see <http://www.nfcworld.com/nfc-phones-list/>

That list contains 305 devices currently on sale.

A free app can be downloaded in order to read the chip.

The EDL is intended to be readable from *at least* 30 ft away. (Cell phones may not have the power to read at that distance however.)

Specialized scanners which operate at higher power can read at greater distances.

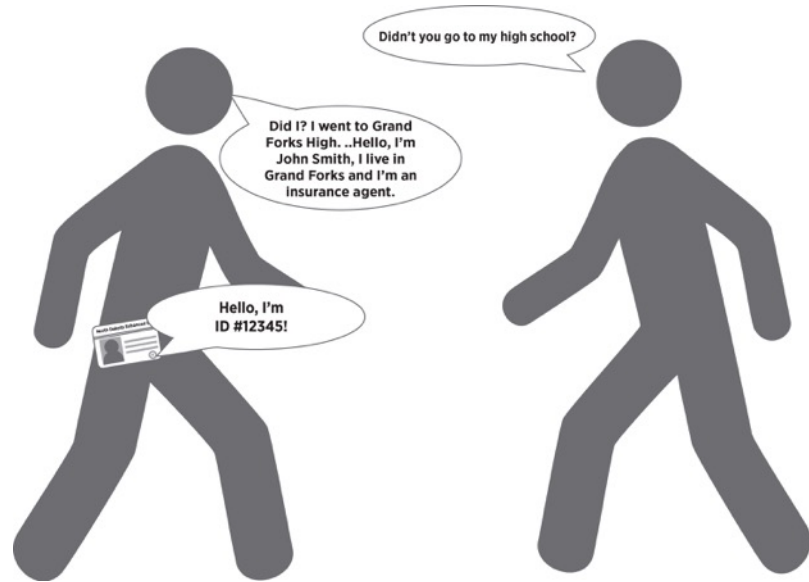
The card can be read through a moving vehicle, allowing road sensors to track users as they drive.



This example here shows how the ID could be associated with a person. An individual engages in conversation with the enhanced license holder, and learns information about him (such as his name, work, residence, etc.)

Meanwhile, his cell phone picks up the EDL chip identifier, allowing that individual to be tracked as they travel.

Identity theft is made easier by knowing some of the places he goes, such as which bank he visits.



The tracking/surveillance is obviously more complete for those with access to the identity database. This would include:

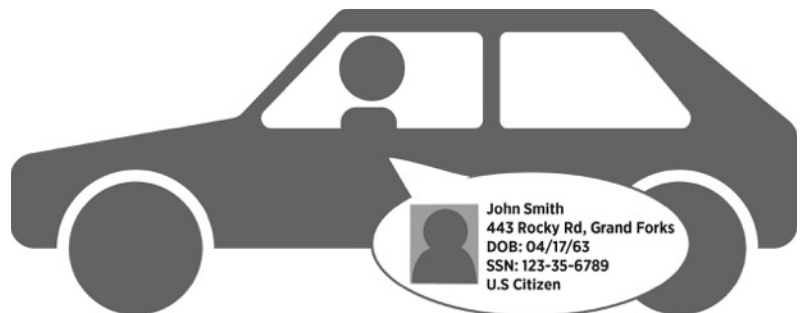
\*US local, state and federal law enforcement

\*Canadian local, provincial and federal law enforcement

\*US and Canadian border control

\*Any individual who has a stolen copy of the above, or illegitimate access to the above via hacking or is using a legitimate user's credentials (username/password)

Since there are so many different entities with access to the identity database, that creates a lot of opportunities for illegitimate access.

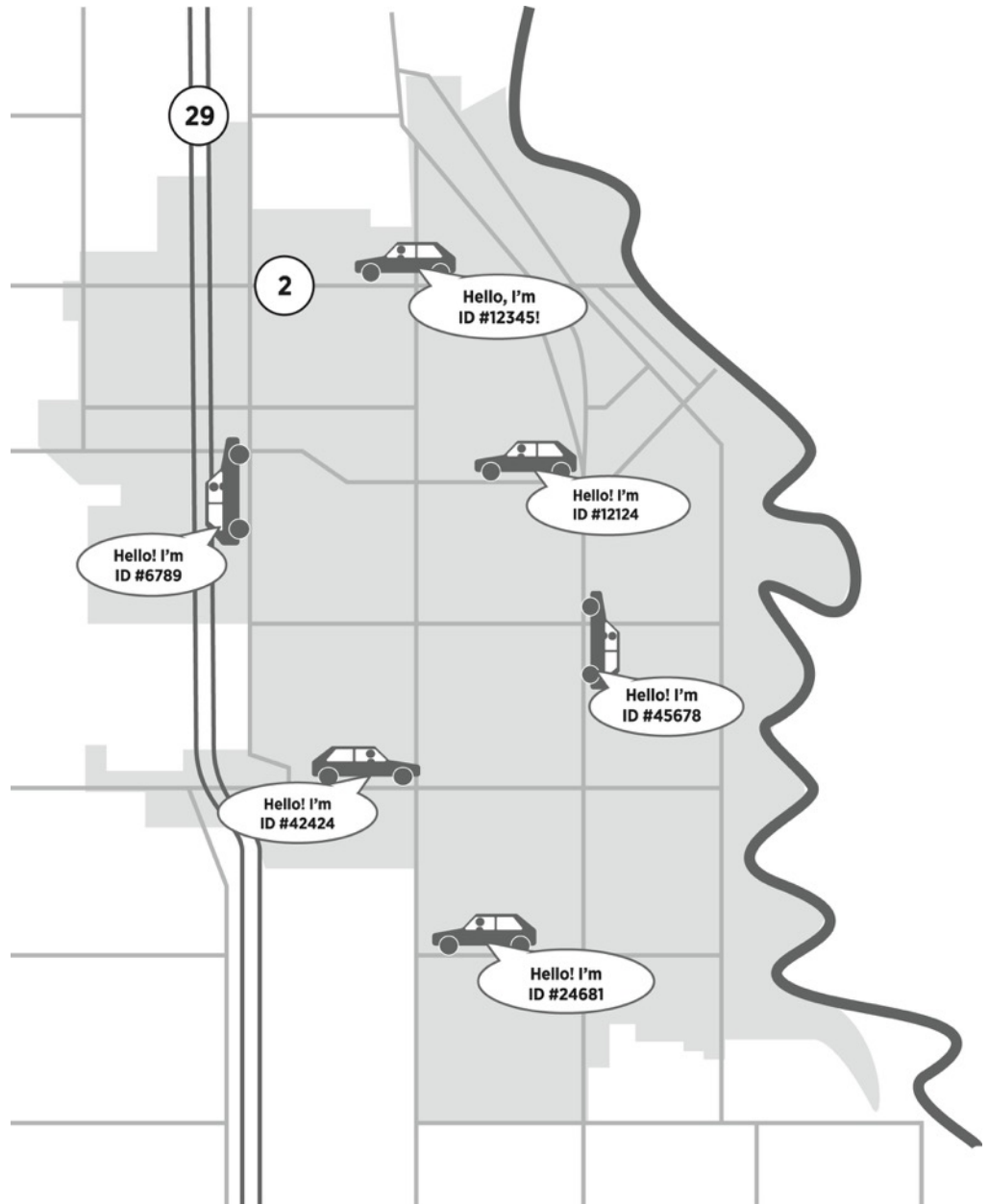




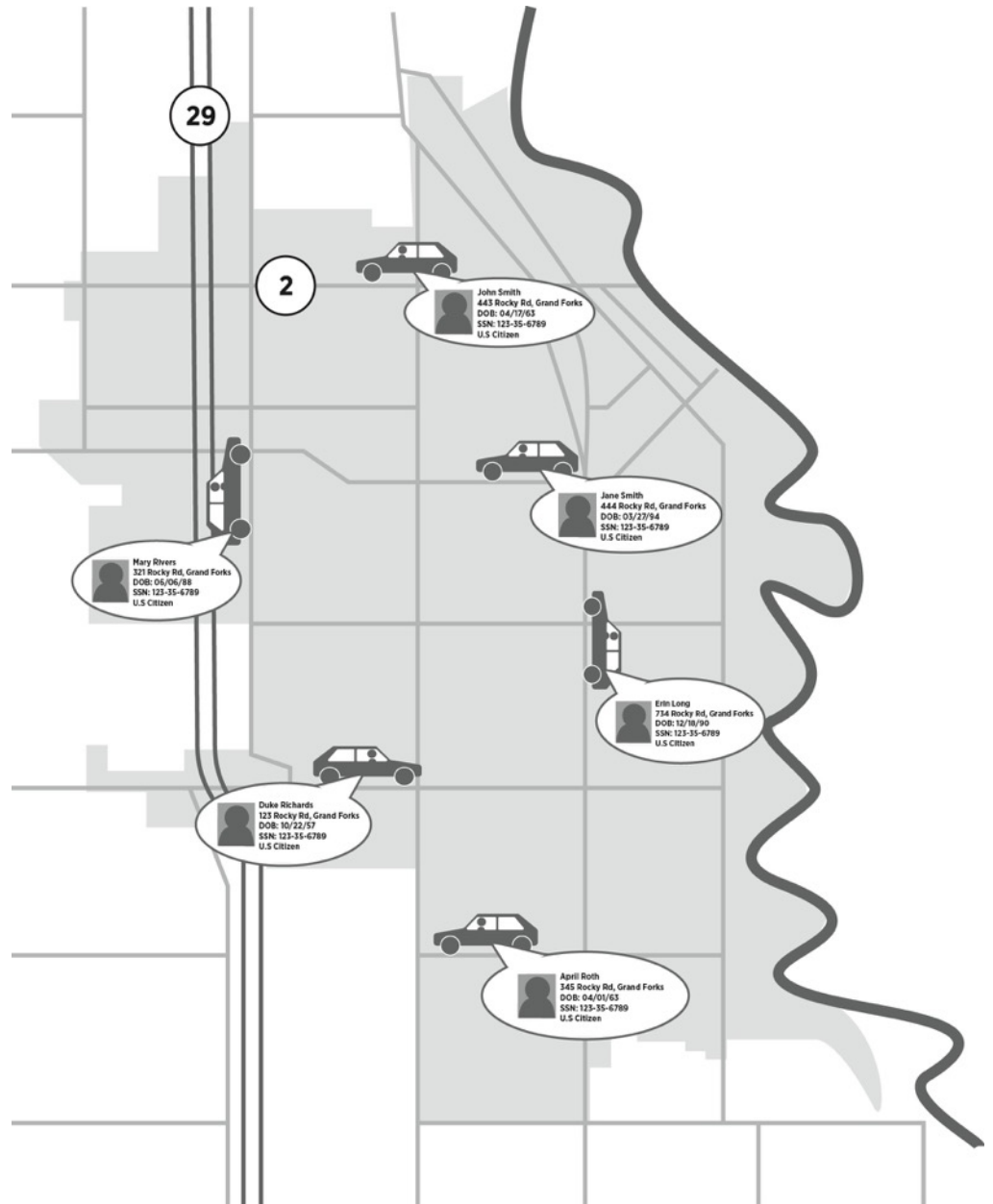
Shown here we see how a network of road sensors could track enhanced license holders as they travel.

Remember, EDL holders are all American citizens, so in addition to the unique trackable ID number, it is always known that the holder is a US citizen.

This is particularly problematic when a citizen travels abroad with the EDL.



Alternatively, if the sensor network were operated by someone with access to the identity database, the tracking data is much richer and more useful.



The problem of tracking is shared with the US Passport Card, but not the US Passport, which has an encrypted chip and includes a metal mesh woven into the cover to prevent low-powered RFID readers from accessing the chip when the passport is closed.

The SB 2148 text contains a line saying “An applicant must sign an acknowledgment of understanding of the radio frequency identification technology and its use for the sole purpose of verifying United States citizenship before being issued an enhanced license, permit, or identification.”

Similar language appears in other states’ EDL statutes.

**If the card is so secure, why does the applicant have to acknowledge the chip?**

I think this language is intended to waive the card manufacturer from liability due to damages from the chip, such as ID fraud. Alternatively it is to warn the licensee that they have to protect the license differently because of the chip.

States currently issuing EDLs include a security sleeve, the text below is from the Michigan Secretary of State’s website:

---

“Why was I given a sleeve for my enhanced license or ID?

Each enhanced license and state ID will be mailed with a special sleeve that can be used to store the card. The sleeve shields your enhanced driver's license or state ID card from unauthorized Radio Frequency Identification (RFID) readers. When you need to access your enhanced driver's license or state ID card, remove it from its protective sleeve. Keep the card in its sleeve when not in use.”

Enhanced License Security Feature/RFID chip  
[http://www.michigan.gov/sos/0,4670,7-127-1627\\_8669\\_53333-213055--,00.html](http://www.michigan.gov/sos/0,4670,7-127-1627_8669_53333-213055--,00.html)

---

Questions:

1.) Why would this legislature approve the issuance of an ID card which is so defective security-wise that *it must be carried in a protective sleeve*?

2.) Why would this legislature approve the issuance of an ID card which is so defective security-wise that the licensee must acknowledge the chip, possibly waiving liability due to damages for the card design?

## **Issue 4: The EDL is compliant with the Federal REAL ID Act.**

My interest in the Enhanced License began in November 2012 when I blocked the Ohio Department of Public Safety's attempt to issue a REAL ID Act compliant license by issuing its own administrative rules. Public Safety was ultimately not successful because it lacked the statutory authority to create the rules needed for REAL ID Act compliance.

This was followed in 2013 by the introduction of an Ohio House bill for the Enhanced License. After the bill passed committee I realized that the Enhanced License granted the authority necessary for REAL ID Act compliance.

It is my belief that the Enhanced License Program is being sold to border/near border states which have rejected REAL ID Act compliance. Indeed, DHS documents imply that the Enhanced License Program is sufficiently similar to REAL ID Act that it would fully accept EDLs as REAL ID Act compliant.

On a DHS website concerning the REAL ID Act:

---

### **May Federal agencies accept my Enhanced Driver's License?**

Yes. State Enhanced Driver's Licenses (EDLs) designated as acceptable border-crossing documents by DHS under the Western Hemisphere Travel Initiative (WHTI) are acceptable for official federal purposes such as accessing a Federal facility or boarding a commercial aircraft.

REAL ID Frequently Asked Questions for the Public  
<http://www.dhs.gov/real-id-public-faqs>

---

In the case of North Dakota, which fully rejected REAL ID in 2007 (SCR 4040), the Department of Homeland Security, in spite of North Dakota's full rejection of REAL ID, has decided that the state's licensing standards are close enough to the REAL ID Act standard to consider it compliant \*at this point in time with an extension granted to fulfill the rest of the standards.\*

This curious state of affairs is by design. States were either completely and unambiguously rejecting REAL ID (like North Dakota) or were taking no action towards compliance. With deadlines passing by, DHS decided to try a phased-in enforcement, counting as many states/license holders as possible to be compliant. This is how North Dakota, a full rejection state, is considered compliant during this phase, and was granted an extension to meet the federal regulations even though it did not ask for one. (<http://www.dhs.gov/real-id-enforcement-brief>)

Hence the push for the Enhanced License: Many states, such as Ohio, Michigan, Minnesota, New York and North Dakota have in their various ways failed to meet the REAL ID act. Michigan, Minnesota and New York now have the Enhanced License, which DHS has decided meet the REAL ID Act requirements. My expectation is that DHS will say that the states are compliant with the REAL ID Act by saying that citizens in those states can/will have to get the EDL in order to use their ID to fly commercially.

**Here is a list of the parties interested in seeing North Dakota adopt the EDL:**

**Federal Department of Homeland Security:** as mentioned before, ND's adoption would allow for another state to be added to the fully compliant column, making it easier to require americans to have EDLs or REAL ID Act compliant licenses in order to fly.

**Federal Law Enforcement:** as discussed elsewhere in this document, the EDL/REAL ID is a federalized document which allows easier access by federal law enforcement to citizen identity records. A central database of citizen identity and photograph records is a key component to the surveillance state.

**Identity card manufacturers:** all on its own, the North Dakota EDL is a minor project (as evidenced by how expensive the card has to be in order to tender a successful contract.) But, again, it allows the state to be considered to be REAL ID Act compliant, and an enforced compliance would require all 50 states to issue the more expensive, more complicated documents. Full national REAL ID Act implementation is worth at least \$4 billion. (<http://www.chicagotribune.com/news/local/breaking/ct-drivers-license-airports-met-20150226-story.html#page=1>)

This is why the legislature received testimony from the Coalition for a Secure License, a non-profit group whose organizational mission is so narrowly focused that I believe it represents the identity card industry.

That industry is dominated by one manufacturer: the US passport, the US passport card and 41/50 states' ID cards, including North Dakota's, are manufactured by the French company Morpho.

Morpho is owned by SAFRAN, a Paris-based defense contractor, which is 25% owned by the Government of France. It manufactures the ID cards and passports for most of the worlds' citizens. It would easily be the biggest beneficiary of full REAL ID Act implementation.

Morpho not only manufactures the cards, it provides the software for the computer systems which operate the identity databases.

# Summary of issues with SB 2148

## 1.) This bill is unnecessary

Few North Dakotans want or need an enhanced license, and those who do would be better off getting the cheaper, longer lasting US Passport Card or the more secure, more useful US Passport.

## 2.) The EDL is a national ID card

The form, content and application of the EDL are dictated by federal rule.

This card commingles the North Dakota license database with federal databases in an irrevocable way.

## 3.) The RFID chip of the EDL is a serious security risk

Offering no benefit to the licensee, the RFID chip of the EDL allows for the tracking of license holders with a variety of inexpensive scanning devices. It also allows for sophisticated tracking of license holders by those with legitimate or illegitimate access to the identity database(s).

The security risks of the document are sufficiently known and acknowledged that other states recommend their citizens to keep the card in a security sleeve.

In an era of increasingly complicated security risks, the state of North Dakota does not need to issue a document with known security defects.

## 4.) The EDL is compliant with the REAL ID Act.

The EDL is a way for a variety of interests to get around North Dakota's refusal to enact the REAL ID Act. With the EDL in place, the Department of Homeland Security will almost certainly consider the state compliant, allowing for full federalization/nationalization of the 50 state licenses.

Submitted by James Moyer  
[james@moyer.com](mailto:james@moyer.com)

May 16, 2017

James Moyer  
Medina, Ohio  
[james@moyer.com](mailto:james@moyer.com)  
330 242 3657

re: cybersecurity issues with H.B. 60, request for audit and amendment

Representatives Hambley and Rogers:

I believe that you have seen the testimony I gave two years ago to the North Dakota House Transportation Committee regarding SB 2148, a proposed Enhanced License program.

The North Dakota House rejected the bill 26-63 due to the cybersecurity issues raised, as well as a fear that the bill would be used to force North Dakota into the REAL ID national identification card program.

In the two years since North Dakota rejected the Enhanced License program, I continue to find the same issues with the proposed bill in Ohio. The federal EDL legislation was written years ago before policymakers became well acquainted with the unique cybersecurity issues of identity cards and identity card systems.

The basic unencrypted chip requirement of the EDL, for instance, is prohibited in international passport documents by the international standards document ICAO 9303, which requires a basic encryption scheme instead. Today many countries use an enhanced encryption scheme in passport RFID chips, and some countries now use advanced elliptic curve cryptography to protect the RFID.

As I noted in my testimony to the Ohio House committee from a couple weeks ago (attached), the bill makes Ohio a franchisee of the US Department of Homeland Security in order to issue an international travel document at higher cost and complexity than those already issued by the US Government. This is not a small government conservative's bill, and the North Dakota House recognized that.

I return back to the cybersecurity issues of the bill, which add complicated interconnections between Ohio's citizen identity database and other computer systems at the US federal, Canadian federal, Canadian provincial, Mexican federal and Mexican state levels. Extra connections into the Ohio citizen identity database increase the likelihood of cyberattack. That is because each new connection is a conduit into Ohio's database, so that the weakest point for Ohio's citizen identity system the weakest of the list above. The bill might make it possible for a cyberattack to come through, for example, the DMVs of Jalisco, Mexico or Quebec, Canada. As we've seen by last Friday's significant cybersecurity attack (Wannacry), a lot of government agencies across the world are operating systems with major vulnerabilities.

Because of this I would ask that your offices suspend the movement of the bill so that it may undergo a cybersecurity audit by the Ohio Attorney General's office/Governor's office. (Perhaps in future the Legislative Services Commission would do this automatically as part of its duties.)

## **Proposed Cybersecurity Amendments**

In addition, if your offices insist on this bill in spite of its issues, I would ask that your offices offer a series of cybersecurity amendments:

- 1.) Require that the words "SECURITY WARNING: Keep in RFID blocking sleeve at all times" be printed on the face of the document. As a person who has studied the security issues of identity cards and identity card systems, I find a lack of security warning unconscionable.
- 2.) Establish liability for a cyberattack of the EDL program, and the minimum liability should a cyberattack occur.

As discussed in a document I gave to the Attorney General's OHLEG advisory committee in 2015 (attached) the likelihood of cyberattack and biometric data loss in the Ohio citizen identity system is such that we need to establish who would be financially at fault for such a failure and by how much.

I believe that the fault should reside with the vendor of the system where possible (which is the implied preference of the new Ohio driver's license system tender.) The state could seek cyberinsurance should it, or one of its interconnections, be at fault.

A minimum liability of \$10,000 per high resolution facial biometric or fingerprint/iris biometric (a potential biometric given the current wording of the statute) would be reasonable.

- 3.) Require that the EDL program be *critical infrastructure* and be compliant with those requirements (NIST Cybersecurity Framework.) Critical infrastructure is the very highest level of cybersecurity protection available on federal and international standards. It also protects the program in international cybersecurity treaties, which prohibit attacks on critical infrastructure. (It is my suspicion that, sooner rather than later, the American citizen identity system will be elevated to critical infrastructure status, this is just protecting the program early-on.)
- 4.) Restrict the biometric to only facial biometric. There is no reason to let DHS be in charge of which biometric Ohioans should have to submit for the program. If Congress wants to change the program and require a different biometric, then the Ohio legislature should have that discussion and amend the statute if they desire. This is particular important if the EDL program becomes Ohio's only REAL ID Act compliant ID.
- 5.) Require that the acknowledgment waiver in 4506.072(A)(3) detail the risks of the biometric enrollment (such as biometric loss) and unencrypted RFID security problems. This would include, for instance, explaining more graphically what the RFID and what devices can read it.

## **Proposed REAL ID Act control amendments**

As indicated in both testimonies attached, this program is in danger of becoming Ohio's only REAL ID Act compliant program, as determined by the Department of Homeland Security. At this point in time, Ohio has a series of exemptions which allow its normal driver's license and state ID card programs to be REAL ID Act compliant. These are in the best interest of the privacy and security of Ohioans.



The danger of the EDL program is that the Department of Homeland Security may certify only the EDL as being compliant with the REAL ID Act. That would mean that only the EDL would be usable for domestic air travel (and that the majority of Ohio licenses would be EDL cards, and not regular licenses.)

Indeed this is already happening, Washington State's EDL program is its state's only REAL ID Act compliant program, and therefore the majority of cards issued in that state. It appears that Minnesota will be moving in that direction.

Given that the EDL program is a cybersecurity morass, this would be a major error for the people of this state (particularly because it gives DHS so much authority to change Ohio's issuance protocols.)

I am not sure how to word this amendment, but the legislation could lock the program so that it is not intended to be Ohio's REAL ID Act compliant card.

Representatives, the risk of cyberattack of the Ohio citizen identity system is real, and this bill makes it much worse. I know it strikes as a rather innocent change, but it's a relatively complicated change to the citizen identity ecosystem, which is fragile. If there is anything I'd want your offices to know about Friday's ransomware attack it's that, for how damaging it was, it was done by amateurs. What professionals, a terrorist organization, or a nation state can do would be profound in comparison.

The people of this state need your offices to assume responsibility for the cybersecurity issues raised in this document.

Warm Regards,

James Moyer

attachments:

- 1.) Communication submitted to the OHLEG Advisory/Steering Committees for August 5, 2015
- 2.) Opposition Testimony regarding HB 60 to the House Transportation Committee

Note: I have authored a wide array of documents on cybersecurity issues of citizen identity systems at various levels of state, federal and international governments. These documents have not been published yet for a wider audience, but they comprise a portfolio which may be. Unattached documents and an index of them are available as a courtesy.

An emerging theme of these documents is *the chronic mismanagement of the American citizen identity ecosystem* at the expense of security. The EDL project will be specifically cited as part of this mismanagement.

## **Opposition Testimony regarding HB 60 to the House Transportation Committee**

### **1.) This testimony is a plea for the status quo in order to stabilize the security of Ohio's citizen identity system**

The complexities of securing Ohio's citizen identity system are increasing, criminals are becoming more sophisticated in their attacks against documents as well as the computer systems which hold citizen identity information. In the last couple of years there were major hacking attacks against citizen identity systems in other countries, which included the attack on the US Office of Personnel Management in 2015, in which 21.5 million US citizen records were lost.

*We must assume that more attacks will occur, and that Ohio's ID systems are potential, valuable targets.*

The process of security these systems is already sufficiently complicated without adding a novel travel document which is unnecessary and already exists in other forms (the US Passport/ Passport Card.)

At it's worst, the Enhanced Driver's License combines the problems of passport fraud and the problems of driver's license fraud. Essentially it puts Ohio into the passport business, and there is no compelling reason for Ohio to get into the issuance of passports.

### **2.) Ohio's future as a security innovator is threatened by this program**

Ohio has recently released the RFP for its next generation ID and driver's license system. Supplement 2 of this RFP introduces world-class security compliance requirements for the vendor for the next generation system. This testimony requests that those requirements play themselves out as opposed to adding new deviations into that contract.

### **3.) HB 60 increases data connections to the Ohio citizen identity system**

*Every new connection to Ohio's citizen identity system presents a new entry point for hackers. Ideally the system would exist entirely on "private backbone" so that none of it is accessible to the wider internet. (Indeed, this was the case for many years prior to the internet.) The plea to put Ohio's ID systems on private backbone is because *we simply can't afford to lose this data.**

HB 60 adds a variety of new interconnections into the citizen identity system: this would include DHS connections, connections to US and Canadian border control agencies, as well as other Canadian provincial agencies, in order to make the Enhanced License work. *These new connections will affect security of all licensed Ohio driver's/ID card holders, not just EDL holders.*

In other words, the security of Ohio's citizen identity system is dependent on the security of all these other agencies. As is the case with computer security, it's the agency with the lowest security level which establishes the overall security of an interconnected system.

#### **4.) Identity card fraud/ID theft is due to overuse which is due to multiple-use ID credentials**

At the core of document overuse is making the document too useful, giving it multiple applications and legal standings. In other words, HB 60 proposes more of the same overuse which has led us to today's ID fraud issues.

The best example of this was Ohio's failed experiment with printing Social Security Numbers on driver's licenses. This experiment began in 1967 and within 10-15 years was known to be a security problem. By the early 2000s the experiment had ended. Extra functionality erodes the security of the document, sometimes severely.

#### **5.) The EDL is not good use of the money**

The US Passport card remains cheaper on a 10 year basis than the EDL. (\$50 for 8 years of an Ohio EDL, \$55 for a 10 year passport card.)

#### **6.) The EDL program requires enormous rule oversight by DHS**

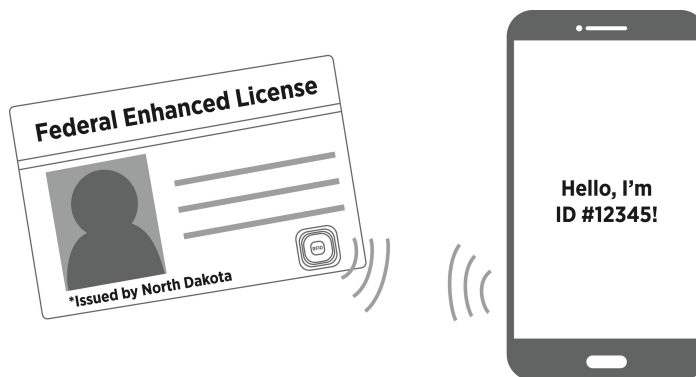
The EDL program is one created in federal law. HB 60 reflects the enormous discretion granted to DHS over its issuance. Arguably Ohio becomes a franchisee of the federal government, for a job the federal government already does with the passport. Why not just let them do it?

This oversight may become a problem later if DHS chooses the EDL program as Ohio's REAL ID compliant card, requiring most Ohioans to obtain it. Last week Washington State approved such a plan.

#### **7.) Unencrypted RFID and easy unauthorized communication with the EDL**

Citizen identity is something which should not be that easy to interact with. There should be physical, time and convenience barriers in place in order to lookup a person's identity. These barriers are essential for the security of the citizen identity ecosystem. Making it faster complicates security. The RFID feature of the EDL is a terrible combination of compromises which value speed over security.

Unencrypted EDLs can be read by NFC capable smart phones (such as the iPhone 6 and 7) with a free app. They are designed to be scanned from a distance of 30 feet, though higher power scanners may scan from a greater distance. At this time DHS has not permitted any state to issue an encrypted EDL, which is why other states distribute EDLs in security sleeves.



But the fact that other states distribute the EDL in security sleeves indicates the severity of the security problems with the EDL. (Indeed HB 60 requires an EDL card holder to waive liability for the security problems of the document and the biometric system.)

**8.) The EDL is part of a misguided effort to internationalize citizen identity cards**

This is best illustrated by Ohio’s adoption of European Union Directive 2006/126/EC.

The small field numbers next to the data elements on the Ohio license are established in EU Directive 2006/126/EC. This directive (law) is intended to standardize driver’s licenses across the European Union.

The applicable text of the directive is below.

DIRECTIVE 2006/126/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
ANNEX I  
PROVISIONS CONCERNING THE COMMUNITY MODEL DRIVING LICENCE

3(d) information specific to the licence issued, numbered as follows:  
1.surname of the holder;  
2.other name(s) of the holder;  
3.date and place of birth;  
4.(a) date of issue of the licence;  
(b)date of expiry of the licence  
...  
8.permanent place of residence, or postal address (optional);  
9.category of vehicle(s) the holder is entitled to drive

1  
3  
9



1  
3  
9



It is not clear why Ohio (and other US states and Canadian provinces) have chosen to standardize the field numbers from the EU directive, but, as a long run trend, this will increase security problems in the identity ecosystem and create complicated legal situations. The Ohio license is best left as a domestic document and Ohioans should get passports for international travel.

<b>Requirement</b>	<b>How Veridos' Solution will address this requirement</b>
<p>The capture of high-quality, consistent applicant portrait images using an automated process that is simple and easy to use;</p>	<p>[REDACTED]</p>
<p>User friendly operating software that require minimal instructions to the applicant from the operator;</p>	<p>[REDACTED]</p>
<p>Capture of high-quality applicant photo images through a high-speed USB connection to the BMV workstation inclusive of the image and associated data to BASS as required to complete the DL/ID process;</p>	<p>[REDACTED]</p>
<p>Integration the signature pad and printer software drivers at each workstation to create a streamlined and unified operating experience;</p>	<p>[REDACTED]</p>