In regards to HB 1072 (Electronic Driver's Licenses)
Opposition testimony to North Dakota Senate Transportation Committee

Chairman Clemens, Committee Members:

My name is James Moyer, I research data protection (security and privacy) of identification card, passport and citizen identification systems. I have twenty years experience in this regard, having delivered testimony and reports to various institutions worldwide, including this legislature, other state legislatures, the European Commission, etc.

The electronic driver's license concept is deeply flawed and unnecessary. I recommend its rejection.

It might seem to you that ID on a mobile app is the answer to a question no one is asking.

So why is this idea being pursued in legislatures from Wyoming to Finland?

The genesis of this product is that it offers identity card vendors a way of monetizing their services differently. Right now ID card companies sell a plastic card product which can be used an unlimited quantity of times for one flat fee. (That is to say, a North Dakota citizen gets a driver's license for $15, and for the next four years, it can be used an unlimited number of times for identification with no extra fee, for either the licensee or the person checking the ID.)

The purpose of the ID on an app is to move from the business of selling ID cards to selling *identity as a service*.

To understand the ID on an app business model, you have to understand its workflow:

1.) The app of the person whose ID is being checked communicates with the ID card company computer;
2.) which communicates with the state DOT computer;
3.) which responds with information back to the ID card company computer;
4.) which then sends that information to the app of the person who is verifying the ID.

This workflow is data processing heavy and involves the ID card company as an intermediary.

1.) Each data processing operation is a billable event;
2.) Each data processing operation creates additional data which has some value to party/parties.

ID on an app allows for charging *per time* that it is used. The charge could vary based on circumstances. Perhaps it could cost $0.50 to use the ID on an app at a local gas station to buy alcohol, $2.00 at a hotel bar and $5.00 to check-in for a flight at the airport. (The fee payer is likely to be the person/entity verifying the person's ID. It might happen on a per event basis, but perhaps it is more likely to occur via a subscription model per authorized device.)

ID via app allows for other monetization opportunities. I have seen proposals from vendors which involve tying the app to other identification functions that a citizen may encounter, such as health care or banking. Perhaps citizens may find this useful, but the inclusion of these other functions greatly enhances the monetization opportunities for the ID card vendor.

However, this creates a lot of complicated privacy and security issues. Many of them are a function of the programming of the app. For instance, does the app ask for or require access to the phone's GPS function? Would the app send this information back to the vendor? Would it send the location information to the state DOT computer? Would the state keep that information in its archive and for how long?

Could the app read the user's contacts or pictures? What would it do with that information?

Another interesting question would be if the vendor integrated Facebook connectivity into the app. Would Facebook receive information regarding the individual's identity? Would DOT receive information about the individual's Facebook app usage? This is a relevant question: both Facebook and the ID vendor have incentives to make this connection. Is that connection in the best interests of the people of this state?

Because of these tie-ins, this legislation establishes a complicated relationship between the citizen and the ID app vendor. One which, as this legislation is currently written, is out of the hands of the legislature since the legislature is giving virtually unlimited rule making authority to DOT. This is a mistake, given the enormous data processing and sharing opportunities this app offers, the legislature should not give up oversight of its functioning. The opportunities for function creep are endless. And much of the decisions regarding how the app works is the discretion of the ID card company.

Showing a plastic ID to a human is a data neutral event. No new data is created. Using this app however would be creating new data in relation to the verification, which needs to be managed, audited and protected (or otherwise deleted.)

Remember, the workflow requires that the ID card company computer has a continuous connection with the DOT computer. That means that the security of DOT's servers is a a function of the security of the ID card company's computers.

Ideally, none of those computers should be connected to the internet (and are connected only by private data lines.) But in order for the mobile apps to work on all these different devices, the ID card company computer has to be connected to the wider internet.

The opportunities for hacking are greatly increased by the prevalence of this app. The apps might broadcast to other apps or be hacked in such a way that the owner of the phone can be positively identified remotely. (I'd strongly recommend that this app not be used by individuals who are police officers, US military service members, employees with security access, etc.)

The truth is that many interests are coming together to get rid of the physical card. While claims today are that there is no interest in eliminating the plastic card, there is little doubt in my mind that the ultimate goal is to eliminate the card (or at the very least, increase the cost of the card.)

This legislature should be aware that, at this point in time, identity card manufacture is highly concentrated in a small number of firms worldwide. None of these are based in the United States, the documents are simply too complicated to manufacture and the patents are largely owned by two European firms (one of which, the French company Idemia, manufactures the North Dakota ID card.) Because they own the patents, it is ultimately up to them if they want to continue manufacturing plastic ID cards and what their cost will be. The state can't compel the manufacture of plastic ID cards given that the state is unable to manufacture the cards on its own. There are more business opportunities in the driver's license as a mobile app than there are in plastic ID cards. The more legitimacy that is given to the mobile ID app model, the faster will be the elimination of the plastic ID cards. Once the plastic cards are eliminated, then the fee per use model will become standard.

For legislatures globally, managing the industry which prints identity cards will be a necessary challenge. Otherwise it will be the industry dictating policy.

There are enormous privacy and security issues with this legislation. As much as I find fault with the plastic ID card security model, I find the ID on an app model to multiply those security and privacy issues significantly.

I would argue that this proposal is unwise, unneeded, and bad value for the citizens of this state.