2011 "(Name of State) Sovereignty Driver License Protection Act"

Provided by the "Stop REAL ID Coalition"

INTRODUCTION and SUMMARY of SECTIONS

The (name of State) driver license uses both facial recognition and fingerprint biometrics (or uses facial recognition biometrics, as is appropriate). Biometrics enrolls U.S. citizens into an international system of identification and financial control over which there is no constitutional authority.

Biometric ID is being used all over the world, creating a global monopoly of power and control, and as such its use violates our First, Fourth and Tenth Amendment rights. This technology is based on international standards so personal-biometric information can be shared globally. The use of biometrics is creating a global surveillance society. Biometrics is commonly used with RFID devices capable of storing and transmitting personal-biometric data, and in many places, these devices are being installed on humans.

It is impossible to uphold the Constitution and protect the rights of (name of State) residents while using biometrics. Therefore, the goals of this legislation are:

- **End the use of biometric identification, for noncommercial driver licenses and ID cards. No fingerprinting (if used) and no facial recognition.**
- **Use lower resolution photographs that will not inhibit the work of law enforcement, but are incompatible with facial recognition.**
- **Remove Social Security numbers from the driver license database after the numbers have been used for child support enforcement.**
- **Protect constitutional rights and our State's rights to issue and control identification documents.**
- **Prevent the use of RFID devices, or similar devices, for driver licenses or ID cards.**
- **Provide adequate funding for the (DMV) and the Department of Human Services for the execution of their duties**

CHANGES TO EXISTING LAW

Each state must summarize the changes to existing law and prepare such a summary for committee hearings, in addition to the detailed summary of proposed legislation. Please see examples of these areas of potential change, in the proposed legislation.

Section 1. NEW LAW

- **Section 1.A.**

Defines implementation date and requires DL/ID card vendor to meet requirements of section.

- **Section 1.B.1-3**

Definitions

1. Defines biometrics
2. Defines noncommercial driver license, learner permit, etc., ex. Class D driver license – hereafter (DL)
3. Defines Identification card

- **Section 1.C.1-2**

Upon effective date, requires the (Department responsible for driver license issuance – hereafter "DMV") to:

1. Cease making biometric comparisons
2. Cease collecting fingerprint images

Section 1.D.1-3

On or before implementation date, the (DMV) shall:

1. Permanently delete biometric fingerprint data from databases
2. Permanently delete Social Security numbers from databases and thereafter, within seventy two (72) hours of (DL) application or identification card application, provide Social Security numbers to the Department of Human Services (Department responsible for child welfare protection enforcement – hereafter Department of Human Services) and then delete from the numbers from the database
3. Render inoperable biometric software, permanently delete such software, not install or use such software thereafter (does not apply to CDL hazmat fingerprinting)

- **Section 1.E.1-5**

Specifies requirements for new facial image collection

1. Resolution - Pixel count of image – (Provides a good image for visual identification but is incompatible with facial recognition) Regarding the lower resolution, Oklahoma

Department of Public Safety spokesman David Beatty said "It provides an image which, though not as clear as the current image, would be useful for visual identification from the driver license and ID card." (May 7th, 2008)

2. Image stored in separate database
3. Image collected using white background
4. Image not to be collected using blue background so lower resolution images are easily distinguished from previously collected higher resolution images
5. Only one (1) facial image can be collected after implementation date. New facial image collected for renewal requires deleting previously collected image, obtained after implementation date. The use of 3-D facial recognition with public surveillance is possible with the collection of multiple facial images. It is therefore necessary to prevent the collection of multiple images.

- **Section 1.F.1-7**

Specifies what the act does not prevent:

1. Collection of biometric data relating to serious traffic offenses or physical arrest
2. Compliance with TSA regulations for hazmat endorsements of CDL
3. Collection of Social Security number for CDL
4. Requesting and receiving motor vehicle or driver license records, but limits sharing of facial image to one image, one name and one record – Access restriction needed to prevent access to database by another entity, such as the federal government, for the purpose of facial recognition searches
5. Administering Sex Offenders Registration Act
6. The collection of compliant facial image by Driver Examiners to be used by agent to verify that the same person that was before the Examiner is the same person being issued a (DL) or identification card
7. Performance of lawful duties by Motor license agent

- **Section 1.G.**

Prevents the use of RFID-RFT technologies

- **Section 2.**

Sets effective date and implementation date