

PROPOSED STATE LEGISLATION

STOPPING REAL ID AND BIOMETRIC IDENTIFICATION

Presented by STOP REAL ID COALITION

Contents

1. Introduction
2. Strategies
3. Proposed Legislation Arranged by Bill Subject
 - A. Ban state participation in the REAL ID ACT of 2005
 - B. Ban the use of all biometrics for state ID and make state photos incompatible with a biometric ID system
 - C. Make state databases incompatible with a biometric ID system, protect religious freedom and privacy
 - D. Protect state databases from illegal searches and data sharing – Remove the influence of international organizations, over state issued ID
 - E. Improve ID document integrity to address legitimate security issues
 - F. Other Privacy Concerns - Address additional religious rights and privacy issues relating to biometrics, ID theft and discourage a future attack on state sovereignty

1. INTRODUCTION

Global ID system

The Department of Homeland Security (DHS) is enrolling the world in a single global system of identification and control. This system is built on biometric identification (ex. facial recognition) and the global sharing of personal and biometric information collected by governments and corporations.

Robert Mocny - Department of Homeland Security (DHS) US-Visit Program -- **stated that** *“information sharing is appropriate around the world,” and DHS plans to create a “Global Security Envelope of internationally shared biometric data that would permanently link individuals with biometric ID, personal information held by governments and corporations.”*

International organizations

Under REAL ID and its proposed rules, DHS requires states to adopt document and photo standards set by two international organizations, the American Association of Motor Vehicle Administrators (AAMVA) and the International Civil

Aviation Organization (ICAO). AAMVA and ICAO are the architects of international biometric driver's license designs and biometric passport designs.

States and global biometric enrollment

States that comply with REAL ID will be enrolling their citizens in the same biometric system used with e-passport, Western Hemisphere Travel Initiative (WHTI), Transportation Worker Identification Credential (TWIC) and the international passport/driver's license hybrid for border-states. Facial recognition is the biometric of ICAO travel documents (e-passport), REAL ID and its proposed rules. Biometric industry tests have proven that facial recognition is highly inaccurate, significantly lower than vendor claims. Therefore, the apparent goal of facial recognition is not security, but complete global enrollment into a single common biometric system of ID and control. Currently biometric enrollment, just for the e-passport program, is 50 million people a year.

Global information sharing

A global biometric system depends on sharing personal-biometric information. Therefore, REAL ID requires states to link databases. Once databases are linked, states lose control over their ID system. Under the "Drivers Privacy Protection Act" (DPPA), DHS can access this linked data system, and potentially share state collected data globally, a plan already endorsed by DHS.

The photos contained in the state system could then be used with facial recognition software. Linked databases using facial recognition would facilitate a borderless global public surveillance system able to identify anyone, anywhere. This is the intended purpose of the software and the data sharing. DHS may also share detailed personal profiling information gathered by data mining, background checks and communications surveillance. Therefore, states must take measures to control the availability of such information and restrict access to the databases under their jurisdiction.

Previous federal attempts

Biometrics and federal standards, for state ID, are NOT exclusive to REAL ID. The federal government has tried to impose biometrics on state ID since 1986 and has tried to impose federal standards on states since 1996. As a result, corrective legislation must address the deeper issues that will resurface again and again, long after REAL ID.

Goals of proposed legislation

The REAL ID ACT of 2005 is part of this global biometric system. State legislation must ban participation in REAL ID, make state database information incompatible with biometrics, incompatible with international ID document standards, make state database only accessible through legal, accountable means totally controlled by the state, not an international organization

collaborating with a state agency. Citizens must also be given more control over the information the state retains, making the database incomplete and less valuable to DHS. (See sec. 3. Proposed Legislation Arranged by Bill Subject)

Beyond REAL ID

Stopping REAL ID and banning biometrics will not stop the threats from AAMVA and future threats from DHS. Many data sharing agreements are already in place between states and AAMVA. For example, REAL ID requires states to participate in the “Driver License Agreement” (DLA), an agreement between AAMVA, Canada, Mexico and states. This data sharing system will exist without REAL ID. States must evaluate all the agreements that govern how personal information is shared with other states, government agencies, insurance companies, etc. and remove the influence of AAMVA from those agreements.

In addition, high-resolution photos make state databases a prize, sought after by DHS, since those photos may be usable with facial recognition. States must reduce photo image resolution so photos are unusable with facial recognition.

These steps are complex and may be expensive. However, that will be the price of maintaining freedom and the constitutional rights of states. Even in monetary terms, these solutions are well below the costs for states to implement REAL ID (23 billion dollars over 10 years).

Addressing the measures below should protect state ID from federal takeover for several years. Future threats would require complete re-enrollment (new photos – new information) and rebuilding document standards. Extending state renewal cycles would also extend the “re-enrollment” process, giving states greater opportunity to scrutinize so-called “security legislation.”

To summarize, it is the responsibility of state lawmakers to protect their citizens from the threat of federal tyranny. The Tenth Amendment expressly grants states such powers, to provide that protection. This global ID system portrays religious freedom, personal security and privacy as expendable rights. Therefore, it is up to states to stand up for liberty and protect those rights.

The First, Fourth and Tenth Amendments to the Constitution

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment X

The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.

2. STRATEGIES

- A. Legislation must be sponsored by members of both parties – this issue touches the lives of every citizen and is not a party specific issue
- B. Draft multiple bills that are germane, but may be submitted to different committees – if one bill is stopped, another may adopt similar language (ex. one bill could address OPT-OUT provisions as a civil rights bill, protecting religious freedom and privacy -- banning REAL ID and biometrics could be submitted as a driver's license bill – document integrity issues could be addressed as an immigration bill, etc.)
- C. Gather support from committee heads to insure a vote on the bill
- D. Rally public support through press releases, endorsements from religious and privacy groups (liberal and conservative) news articles and TV interviews – Global data sharing and a single global ID system touches everyone, so an informed public will support this change –

Make the case simple- *“REAL ID will enroll U.S. citizens in a global biometric ID system designed by international organizations. DHS has indicated its intentions to share personal-biometric information globally. We therefore oppose REAL ID, biometrics, database linking, global information sharing and the influence of international organizations (AAMVA and ICAO) on state and federal laws.”*

3. PROPOSED LEGISLATION

- A. Ban state participation in the REAL ID ACT of 2005**
- B. Ban the use of all biometrics for state ID and make state databases and ID photos incompatible with a biometric ID system**
 - 1. Ban the use of all biometrics for state ID – STATES MUST DETERMINE IF THEIR MOTOR VEHICLE DEPARTMENT IS USING FACIAL IMAGE RECOGNITION – To many lawmakers and to the public, a digital photo ID is not a biometric - Many state motor vehicle departments have implemented facial recognition without the knowledge of their lawmakers or the people

2. Recollect any shared biometric information and wipe state databases of all stored biometric information such as fingerprints -- High resolution facial images, used with facial recognition (such as Oklahoma or Illinois), can either be wiped from the state databases or states can use an image “degrading” software to reduce the pixel count of the image to the new specified resolution levels (see item 3) – a permanent data wiping algorithm must be used when wiping all biometric fingerprints and high resolution facial images (see TECHNICAL NOTES below)

NOTE: Recollection of data is extremely important, since personal-biometric information may be backed-up by DL/ID card supplier (ex. Viisage-L1).

3. Photos MUST be low resolution images, with a maximum of 24-27 pixels between eye centers -- IMPORTANT: All digital photos can be used with facial recognition software, but high resolution photos increase accuracy – REAL ID (ICAO standards) photo standards call for 90 pixels between eye centers – see *TECHNICAL NOTES below* – 24-27 pixels between eye centers provides a good image for “human” ID verification, but is too low for effective facial recognition

Changing photo resolution is the most technically challenging issue, but is the most important issue for protecting the future of state ID

4. To prevent future use of biometrics, each state must consider how to deal with existing equipment and software. States can require the liquidation of biometric equipment and software packages (ex. digital fingerprint scanners, high-resolution camera equipment, facial recognition software package, ex. Viisage/L1 ID Solutions- FaceEXPLORER) – Some states may wish to pursue litigation or negotiation with a facial recognition supplier on grounds of misrepresentation of product performance – see 2003 International Biometric Group Report (IBG) on facial recognition performance in large database environments

IMPORTANT NOTE: Biometric equipment-software is very expensive. However, all facial recognition software must be wiped from state databases. Objections to this can be reduced by inquiring of the licensing agency as to the “real-world” results compared to vendor claims and actual prosecutions against those who have obtained multiple DL/ID cards under different names. (see 2003 IBG report for expected results). Real world tests will prove that the licensing agency purchased a product that

did not work. Having these questions and answers BEFORE drafting legislation will give lawmakers added leverage to remove facial recognition software since the product WILL NOT meet vendor claims, the agency DID NOT test to prove vendor claims or blindly accepted vendor claims. Regardless, the agency and the vendor cannot justify the continued use of the facial recognition product.

Biometric fingerprinting has a higher accuracy rate than facial recognition. Some lawmakers may not fully understand the constitutional reasons for ending its use or the necessary liquidation of fingerprinting equipment and software. Therefore, an alternative to liquidation is to make fingerprinting voluntary. Voluntary fingerprinting must be a conscience OPT-IN and NOT based on employee persuasion or deceitful representation. Applicants must make their decision on a true representation and understanding of the technology. In a separate place on the DL/ID card application, an option similar to the following could be added.

[] I voluntarily submit to biometric fingerprinting. I understand that biometric fingerprint images are compatible with international biometric fingerprint standards. These standards permit the sharing of biometric information internationally. I understand that biometric technologies can be inaccurate and therefore, there is a risk that I may be incorrectly identified using this technology

5. Authorize 3rd PARTY SUPERVISION – verify database wiping and photo resolution compliance with motor vehicle agency and DL/ID card vendor
6. OPTIONAL LEGISLATION - Extend the renewal cycle of the DL/ID card (6-8 years). This will dramatically extend the enrollment process for any new federal law similar to REAL ID
7. OPTIONAL LEGISLATION -- Law enforcement officers shall not collect biometric data from individuals unless the individual is charged with a crime justifying incarceration – i.e., no mobile biometric scans or photos for biometric identification (ex. Florida, Kansas) - No public surveillance cameras linked to criminal databases (ex. Florida, California) – Persons found innocent of a crime, or not charged with a crime after being detained, may request to have their biometric information removed from the system (wiped) – Persons under arrest must be notified of these rights
8. For states using biometrics, corrective legislation must require the immediate suspension of all biometric activity (use of facial recognition

software, collection of fingerprints, etc.) between the date of legislation passage and its effective date

- IMMEDIATE RELIEF

- A. In many cases, enrollment into a biometric ID system violates religious beliefs. If applicable, the public must be notified of a change in the law and motor vehicle departments must provide a means for immediate relief (immediately wiping all collected biometrics and high resolution photos from the state database and archives of the state database)
- B. Use DL/ID card applications for INSTANT OPT-OUTS and DL/ID card address options (DL/ID CARD options), providing instant change to existing biometric status of cardholder (i.e. after individuals are informed of change in the law, they can elect to immediately have their biometric ID-photos-SSN-etc. status, changed in the motor vehicle record)
- C. There must be a means for wiping biometric information (ex. fingerprints or photo images), or degrading existing photo images so they cannot be used with facial recognition biometrics, collected during the transition between law passage and implementation. Option -- no photo shall be "retained" by motor vehicle agency between law passage and effective date requiring agency compliance, including back-ups and archives

- TECHNICAL NOTES

- A. Database wiping of biometric information

Data wiping must be permanent and supervised so that the information can never be retrieved (ex. inclusive of scheduled back-ups and disaster recovery mirror systems). Deleted biometric information can potentially be recovered, so data wiping is the only way to securely remove existing data. Typically a "wiping" algorithm wipes the same space several times using different characters or blocks of information, so that the wipe is permanent. Examples of these algorithms include:

- i. Super DOD 5520.22-M (Dept. of Defense -13 passes)
- ii. Schneier's Algorithm (overwrites 0xff, then 0x00 then 5 times passes with random data)
- iii. Gutmann's Algorithm (removes magnetic traces)

NOTE: It may be necessary to destroy CD/DVD storage media containing biometric data since such storage media cannot be effectively wiped using conventional methods.

B. Photo Resolution - Technical requirements

- i. Photo image resolution shall be suitable for human identification and verification but unsuitable for facial image recognition. Uncompressed photo images shall have a maximum resolution of the full image of 48 pixels of resolution for the width of the head, and correspondingly roughly 24 pixels from eye center to eye center. This corresponds to a minimum full image width of 84 pixels and an image height of 105 pixels.
- ii. For a photograph with head width roughly 0.78 inches, the scanner resolution shall not exceed 60 dots per inch.
- iii. For a photograph with head width 0.5 inches, the scanner resolution shall not exceed 100 dots per inch.
- iv. For a photograph with head height (from chin to crown) of 1 inch (25mm), this in turn corresponds to a head width on average of 0.8 inches using a typical head geometric ratio of 4 to 5. This corresponds to a required scanner resolution of 60 dots per inch. Therefore when color scanning supplied paper photograph portraits of conforming dimensions using a scanner, the color scanner resolution should be set, not to exceed to 105 dpi.

- **Changing photo resolution will require changes to existing, or new, DL/ID card software. Changes MUST BE PERMANENT. Older digital camera equipment will probably be sufficient to supply the required low-resolution images specified.**

C. Make state databases incompatible with a biometric ID system - protect religious freedom and privacy

1. Allow "Valid Without Photo" ID to be issued for those seeking religious exemptions from photo ID – *(ID verification still depends on non-photo "breeder" documents - affidavits can be used to confirm identity, signed by others who verify identity of the applicant - signature verification can also be used to verify identity after the DL/ID has been issued, law enforcement can easily verify the validity of a Non-photo ID)*

NOTE: It is extremely important to make allowances for all religious beliefs – Once a religious belief is marginalized, ALL religious rights become

subject to government approval, at which point, they become tolerated privileges, not rights! The “MAKE NO LAW...” provisions of the First Amendment must be upheld, regardless of the size of the religious sect. The arguments of a photo being necessary for “national security” are ineffective against a religious right, especially when there are numerous other means of verifying identity without a photo, such as signature verification and additional ID documents, and ALL photo ID documents are based on “non-photo” breeder documents.

2. DL/ID CARD options – protect religious rights, privacy and make state databases incomplete and incompatible with “REAL ID” requirements, thus making the state database less of a “prize” for federal take over
 - A. Allow “Valid Without Photo” and “Valid Without Signature” ID to be issued for those renewing by mail, who are unable to appear in person for renewal
 - B. Permit citizens to OPT-OUT of state retention of Social Security Number, when collected to comply with state or federal law (ex. New Hampshire) - NOTE: The mandatory collection of this number, to comply with a federal law, may violate the Tenth Amendment (states’ rights) – The OPT-OUT legislation should include a requirement to shred the original paper application after the license is issued.
 - C. Permit citizens to OPT-OUT of state retention of photo after issuance of driver’s license (ex. New Hampshire) - May require visiting issuing agency when renewing
 - D. Permit use of mailing address DL/ID card (ex. New Hampshire)
 - E. Redesign application with “options” (ex. New Hampshire)
 - F. State motor vehicle departments must provide written and oral notification of new rights under corrective legislation (see OPT-OUTS and IMMEDIATE RELIEF)

D. Protect state databases from illegal searches and data sharing – Remove the influence of international organizations, over state issued ID

1. Ban state database linking - Lock down state databases containing personal information so that information cannot be shared or accessed without accountability and without due process – DO NOT SHARE DATA WITH DATA MINING COMPANIES - (A careful examination of all points of

access and sharing must be evaluated – ex. auto makers, insurance companies, reciprocal agreements with other states, CDL sharing,

2. Identify all programs, contracts, agreements, etc. involving the state and AAMVA (ex. DLA, DLC, NRVC etc.) – Renegotiate all agreements with states and other jurisdictions so that information sharing for CDL holders, traffic violation records, outstanding warrants, etc., are shared DIRECTLY with each jurisdiction and NOT through a database access system like “AAMVAnet” or a DHS link or portal --All data sharing must be accountable to specific persons and identify the reasons for the inquiry.
3. Stop funding to AAMVA
4. Do not accept federal funds for state participation in AAMVA programs (ex. DLA – see above regarding identifying all AAMVA programs)
5. Do not scan breeder documents or store breeder documents in database
6. Motor vehicle/law enforcement officials must be prevented from communicating with AAMVA regarding the use of biometrics or other technologies that violate new DL/ID laws (i.e. cannot collaborate to re-introduce biometrics)
7. State officials must not accept retain or distribute, documentations or communications from AAMVA, that addresses the issue of biometrics or international ID standards
8. Employ third party to verify motor vehicle and law enforcement compliance - State laws must not rely on motor vehicle agencies to promulgate regulations - Many state biometric DL/ID card laws are a direct result of state motor vehicle department’s relationship with AAMVA and do not represent the wishes of the people or lawmakers
9. NOTE: There are many legal considerations for states using biometrics -- The use of an international biometric ID system and potential database sharing, present a direct threat to many religious beliefs - States may be subject to civil rights lawsuits if they retain the use of biometric technologies or comply with REAL ID --Failing to protect database information may also result in litigation regarding Fourth Amendment privacy rights. Retaining biometric technologies will make states the target for future federal take-over similar to REAL ID

E. Improve ID document integrity to address legitimate security issues

1. Improve ID document integrity – Biometrics has nothing to do with document integrity – Many issues, that prompted REAL ID, can be addressed with improved document integrity -- BIOMETRICS DO NOT MAKE AN ID DOCUMENT MORE SECURE
2. If a state deems it necessary to verify breeder documents, it must do so ONLY through the issuing jurisdiction (ex. Social Security Administration) and NOT through a DHS or AAMVA program -- DHS programs like “Basic Pilot” can be used as data collection sources for DHS, AAMVA etc. Direct verification of breeder documents is the only way to prevent illegal data collection by DHS, AAMVA, and others. Many new immigration laws requiring or allowing document verification through a DHS data clearing point (ex. Basic Pilot) must be revised to allow only direct document vetting with the issuing jurisdiction -- Non-citizen documents must therefore be vetted directly with the State Department or other appropriate jurisdiction

F. Other Privacy Concerns - Address additional religious rights and privacy issues relating to biometrics, ID theft and discourage a future attack on state sovereignty

DHS is gathering information on almost everyone from every possible source, openly declaring anonymity as dead. The “guilty until proven innocent” mentality is dangerous. Therefore states must take measures to prevent ID theft, data mining, and public use of biometrics that potentially violate the rights of individual citizens.

Government Considerations

1. Do not require last four digits of one’s Social Security Number (SSN) for voter registration or SSN for other public documents such as marriage licenses, professional licenses, etc.
2. Minimize information stored in DL/ID barcodes, limiting data harvested by merchant card swipe, or ban card swiping (see “Private Sector”)
3. Prevent schools from collecting biometric information
4. States must not sell personal information of their residents
5. Ban use of RFID or embedded chips from state issued ID

6. Immigration laws must only require SSN or other ID numbers to be verified directly with the issuing agency and not retained by state agency or verified through a DHS-AAMVA, or other database

Government and Private Sector Considerations

7. Decrease consolidation of power, contained in the driver's license, by making other documents useful for identification i.e. merchants, vendors, schools, etc. must accept alternative ID forms to the DL/ID card – REAL ID consolidates so much power in one document and then removes control of that document from the states – adding additional ID documents for public acceptance, reduces the future threat of laws like REAL ID (ex. using a birth certificate or military ID as primary ID for opening a bank account or cashing a check – such legislation may depend on improving the integrity of these “added” primary ID documents)
8. Requests for SSN must indicate by what authority the information is collected and if it is mandatory or voluntary - Almost all ID theft occurs electronically, not through the use of fraudulent documents - Any entity requesting a SSN must indicate by what authority they request the number (Privacy Act 1974) - If a SSN is NOT required by law, then the entity must make goods or services available to those who withhold their SSN. If not required by law, the “application” or document requesting the SSN, should indicate “optional” (ex. medical information, application for employment, banking - when opening a non-interest bearing account, utilities, etc.)
9. If a SSN must be verified electronically, the verification must be done directly through with the issuing agency and not through a third party. Ideally, once the number is verified, the number itself is permanently removed from the system. In this way the prospect of ID theft is reduced and privacy is preserved. This concept can potentially be applied for purposes of credit, government ID, etc.
10. Legislation needs to address public surveillance cameras, informing the public of the purpose of the camera (street level sign near camera or near building access informing public of the purpose of the camera, who is collecting the images and if images are used with biometrics)

Private Sector Considerations

11. Require credit agencies and data mining companies (Choice Point, Lexus Nexus, Axiom, etc.) to inform state residents when their personal information has been “shared” and when credit information has been

requested, empowering people to stop ID theft (notification could be by email, mail, etc. but must not contain SSN in the correspondence) NOTE: The “intelligence community” can obtain personal information from data mining companies without going through the courts, so states must NOT SHARE INFORMATION WITH DATA MINING COMPANIES

12. Require businesses and public services, like hospitals, that collect biometric ID to notify individuals of that collection and provide an alternative form of ID – (ex. birth records, employee ID) - Require businesses that use biometrics in surveillance to post public notification (ex. Las Vegas hotels – Casinos, etc.)
13. Pass laws preventing the scanning of DL/ID cards by retailers for the purpose of data mining. Clearly mark DL/ID cards “DO NOT SWIPE BARCODE” as an option to protect privacy (note: some retailers “require” DL/ID to be swiped when writing a check)

112407 PROPOSED LEGISLATION by bill subject.doc