REAL ID-BIOMETRIC FACT SHEET and PROPOSED LEGISLATION

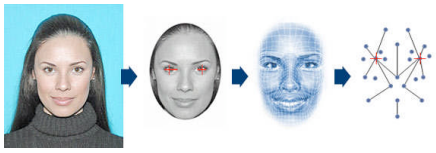
The Final Chapter in a Systematic Plan for a Single Global Biometric ID System

Submitted by the STOP REAL ID COALITION – an association of concerned citizens

CREATING A GLOBAL BIOMETRIC ID SYSTEM

After 9/11, Congress passed many pieces of security legislation. The REAL ID ACT of 2005, for example, sets federal standards for state driver's license/ID cards (DL/ID cards). However, REAL ID is not about 9/11 or stopping terrorism. Like many other federal programs REAL ID is about biometric enrollment.

Biometrics relies on computers to automatically identify individuals based on unique physical characteristics. Many nations, states, municipalities, organizations, schools and businesses are already using biometrics, like facial recognition, digital fingerprinting and iris recognition. The result is a slow methodical global enrollment process, filling databases with personal-biometric information.



Digital images are made up of pixels, blocks of information and color. Image quality (resolution) improves with the pixel count, just like HD television. Facial recognition uses pixels to pinpoint the eyes, crop the face, identify unique facial features and map those features to create a geometric facial pattern. Higher resolution images improve facial recognition accuracy.

Robert Mocny (Department of Homeland Security, US-Visit) 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."*[i]

THREATS TO FREEDOM

The Department of Homeland Security (DHS) is creating a global biometric system of identification and economic control, so that biometrics becomes the common international denominator identifying us to *"governments and corporations."* However, such a system destroys national sovereignty, removing control of the people over their government. This system threatens religious freedom, privacy, states' rights, the rights of representation and our ability to redress grievances, state sovereignty and national sovereignty.

Global information sharing, that affects all Americans, violates the Fourth Amendment and could produce an ID theft pandemic. As *"governments and corporations"* build economic systems tied to biometrics, ID theft would permanently destroy those systems. If a "PIN" number, or Social Security Number (SSN) is compromised, they can be changed. But, one cannot replace a face, a hand or an eye (used for biometric ID). Any compromised biometric-economic system, becomes instantly useless.

A global ID theft pandemic presents legitimate religious concerns, since it could result in a new technology for identification and financial control, such as "'Somark's RFID "tattoo" or as some call it, RFID "mark." This technology stores data and transmits personally identifiable information. It is placed on the skin, rather than under the skin, like a standard RFID chip. To many Christians, such technology may be the "mark of the beast" depicted in biblical prophecy (Rev. 13:16-17). This passage describes a universal system, applying to "all," that links one's body to the control of financial transactions (like biometrics). Therefore, biometrics and global information sharing threaten the religious beliefs of millions of Christians.

Biometrics represents a complete disregard for all religious believes. According to AAMVA's website, religious rights are on a "COLLISION COURSE" with so-called, security concerns. To accomplish complete biometric enrollment, many states have pulled or denied religious exemptions, for "valid without

photo" DL/ID cards. This action threatens the beliefs of Mennonites and some other small religious sects. Many Jews strongly object to biometrics' ability to "catalog" humanity, as occurred during the Holocaust.

Also, under REAL ID, control over the DL/ID card will pass from states to the federal government and the international organizations running the biometric and data sharing system. This violates the Tenth Amendment, which limits federal powers, and retains more direct powers for state control where the people have far more access to elected representatives. This access protects representation. Under REAL ID, the people have no representation with those who control them and once data is shared, there can be no redress of grievances (First Amendment). As a result of these threats, the most liberal and most conservative have found common ground to defend their civil rights. DHS understands these threats to constitutional rights and has therefore resorted to deceit, rather than transparency, perpetrating the ultimate betrayal of public trust.

9/11 – GREEN LIGHT FOR GLOBAL ID IMPLMENTATION

The creation of such a system has nothing to do with 9/11 or terrorism. 9/11 provided the opportunity to fast-forward federal plans for biometrics and linked databases that first began in 1986[ii] and to force an international biometric passport and biometric ID standard on other nations that began in 1995[iii].

To create this system there must be:

- Enrollment – DL/ID, passports, military ID, etc.
- International biometric and document standards to ensure global sharing
- Linked databases providing global access to personal-biometric identification data, financial information, medical information, demographic information, etc. (profiling)

The three main entities driving this system are:

1. The American Association of Motor Vehicle Administrators (AAMVA)
2. The International Civil Aviation Organization (ICAO)
3. The Department of Homeland Security (DHS)

AAMVA is an international association of motor vehicle and law enforcement officials[iv]. AAMVA is responsible for international biometric DL/ID card standards and an international information sharing agreement, the "Driver License Agreement" (DLA)[v]. The most recent AAMVA DL/ID standard is the 2005 "*Personal Identification – AAMVA International Specification- DL/ID Card Design*.[vi]" This DL/ID standard, the DLA and other document standards are requirements, cited in REAL ID HR418[vii] and/or REAL ID "Notice of Proposed Rulemaking" (NPRM)[viii].

Currently, most states share information through AAMVA, instead of sharing directly between states. Compacts govern how and what information is shared. However, states MUST join the DLA to comply with REAL ID. **The DLA will link state databases with Mexico, Canada and other nations that join the DLA.** Therefore, state participation in REAL ID violates the U.S. Constitution's Article 1, Sec. 10 that prevents states from entering into compacts or agreements with a foreign power. AAMVA's influence over international, federal and state DL/ID card laws is undeniable. AAMVA is mentioned 30 times in NPRM and 150 times in REAL ID final rules of January 11th, 2008 [viii]. **Under REAL ID, State DL/ID cards provide enrollment and AAMVA provides the document and database linking system needed for global biometrics.**

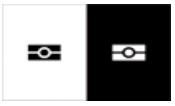
ICAO monitors international travelers, designed the biometric "e-Passport[ix]" (required for "Visa Waiver Nations[x]" and used by the U.S.) and is an agency of the United Nations (UN)[xi]. Pressure from the U.S. has forced many nations to adopt the ICAO e-Passport system so that global enrollment into e-Passport has reached 50 million annually[xii]. The e-Passport

ICAO Logo – ICAO is part of the UN

document stores personal-biometric information in its RFID (Radio Frequency Identification) chip. REAL ID photos comply with ICAO "**biometric data interchange formats**" [xiii] (same as e-Passport), making state photos compatible with global facial recognition standards. These "interoperable" standards serve the purposes of global control and surveillance.

Once this system is fully implemented, it will not matter if one has an Oklahoma or Washington driver's license or EU or U.S. passport, the ID system is the same. Biometrics provides the foundation for programs like the Security Prosperity Partnership (SPP), North American Union (NAU) and NAFTA Super Corridor that are dependent on a common ID system.

ICAO's Biometric e-Passport Logo – visible on the EU and US passports pictured below



DRIVER'S LICENSE or PASSPORT =GLOBAL BIOMETRIC ENROLLMENT

Driver's License with Facial Recognition Biometrics

Enhanced Driver's License - Facial Recognition - RFID chip – used as a DL/ID-passport for border-states

ICAO's Biometric ePASSPORT, with RFID chip used by EU, U.S. & all Visa Waiver nations

DHS - The driver's license is the most powerful document we have, controlling our ability to buy, sell and travel. Federal agencies want this power but must first dismantle states' rights, protected by the Constitution. DHS and other agencies, already have "legal" access to state database records under the "Driver Privacy Protection Act of 1994" (DPPA). However, before wholesale access can occur, states must adopt common document and biometric standards, storing and sharing significant personal-biometric data.

States use AAMVA, and are given grant money, for data sharing through AAMVAnet. States are being prepared for more federal information gathering needs by collecting and sharing personal information for federal laws and programs such as Selective Service enrollment (with SSN), E-Verify, child support enforcement (with SSN), etc. But, REAL ID finishes the job of preparation by standardizing state document and biometric data and imposing an international data sharing system on states, through AAMVA's DLA.

DHS has at least two backup plans if REAL ID is repealed.

- **CONTROL THROUGH NEW LEGISLATION** - Allow state involvement in rulemaking. Keep biometric-compatible photo standards. Require states to meet the standards (ending states' rights). Keep AAMVAnet and give states grant money for DLA participation.

- **CONTROL THROUGH THE DL/ID CARD VENDOR** - Impose REAL ID, document and biometric standards, through the driver's license vendor. This requires having only one vendor, in this case, L1 Identity Solutions (a merger of Viisage and Identix). L1 is involved in passport production and, with its recent acquisition of its only real competitor, Digimarc, will own 95% of the state driver's license market. L1 also owns McClendon and SpecTal, intelligence contractors to U.S. intelligence agencies.

Despite L1's checkered past regarding Viisage's exaggerated performance claims and corruption, L1 has a CLOSE relationship with the federal government, receiving millions of dollars in contracts. This is no surprise considering its Board Members and employee roster are filled with ex-government security officials. Intelligence gathering, biometric DL/ID card design and even passport production are now under one roof, L1. This convenient relationship between the federal government and L1 fits well into DHS plans for real time surveillance-identification and threat assessment of individuals. As the de facto issuer of DL/ID cards, L1 can impose its REAL ID-like biometric "product," on states, and work with AAMVA and DHS to fulfill REAL ID goals.

THE DEPARTMENT OF HOMELAND SECURITY—PROTECTION OR DECEPTION?

After issuing the NPRM, DHS released "20 Questions and Answers"[xiv] about REAL ID. In it, DHS denied:

- Creating a national ID card
- Creating a national database on applicants
- Requiring biometrics for state ID or storing biometric information from state ID

DHS claims are deceitful. REAL ID is an INTER-national ID. Once state databases are ready for global sharing, DHS can exercise its "legal" rights to access state databases, under the outdated DPPA, and harvest state collected information through AAMVAnet (described as the "backbone" of the system).

The most significant "security" legislation written since 2001 has, as its "backbone" an international organization, over which U.S. citizens and their elected representatives, HAVE NO CONTROL.

DHS denies that REAL ID requires biometrics but the NPRM requires that state photos are compatible ICAO 9303 "**biometric data interchange formats"** (same as e-Passport) and the **"Privacy Impact Assessment for REAL ID ACT"** (March 1, 2007) clearly states; "*In addition, as a result of the Act, state databases will contain **standardized photo** images that will **allow law enforcement agencies to use facial-recognition technology** to help apprehend criminals, and the state DMVs will be able to use the images and application data to prevent drivers whose licenses have been revoked in one state from obtaining them in another."* [viii] (emphasis added) **- Law enforcement WILL be using facing recognition on DL/ID databases.**

DPPA would also permit the sharing of state records with the FBI, to fill its new BILLION DOLLAR biometric database. REAL ID DOES require photos compatible with facial recognition biometrics and any government agency accessing the linked database system can use any state collected photo with facial recognition software, making it a biometric. **The federal agency designed to protect us is deceiving us.**

STATE AND FEDERAL AGENCIES – OUT OF CONTROL

REAL ID is a symptom of a society that has lost control of its government, where international organizations have more influence over state and federal law than the people, or their elected representatives.

How can something like this happen? It is common for state and federal bureaucratic agencies to create the rules of a specific law. These rules are seldom reviewed or "approved" by elected officials. In the case of identification, we have two international organizations (AAMVA-ICAO) that have strong influence over the rules. DHS can easily "hide" its international intentions deep within those rules and within the policies, procedures hidden within the international organizations, themselves. This is why most state and federal oversight committees have missed these facts and, thereby, placed us in this dangerous position.

REAL ID and biometrics are the direct result of unsupervised, out of control, state and federal bureaucratic agencies, influenced by international organizations, like AAMVA and ICAO. For example, many state DMV's use facial recognition without the knowledge of the Legislature or the people. On March 1st, 2007 DHS issued REAL ID's "Notice of Proposed Rulemaking" (NPRM), revealing REAL ID's global biometric connection[xv] through a single footnote and references to AAMVA.

FACIAL RECOGNITION – The Global Biometric of Choice – Key to Global Surveillance

Why Facial Recognition? Facial recognition can use existing digital photo databases, so that enrollment occurs without the individual's knowledge. AAMVA commissioned the "International Biometric Group" (IBG) to evaluate biometrics in a database of 300 million.

The 2003 report revealed:

- *Facial recognition can be used to acquire faces from static camera or video sources*
- *Facial recognition databases can be created from images not originally collected for biometrics*

Facial recognition can be used for public surveillance. Facial recognition can be used on practically ANY digital facial photo or captured facial image including Closed Circuit TV (CCTV). Public surveillance is on the rise, like Great Britain with an estimated 500,000 surveillance cameras in London and 7 million nationally.[xvi] DHS is spending millions on 3-D facial recognition testing and high-resolution surveillance cameras. WHY? Unlike common 2-D DL/ID photos, 3-D facial recognition accounts for changes in facial angle and lighting and therefore has only one purpose, public surveillance.

In addition, DHS is collecting, buying (data mining) and storing huge amounts on average citizens, creating the most intimate personal profiles. Flying commercially may trigger a background check that reveals, medical, financial even sexual information about individuals. Potentially, this information can be used when individuals are identified in public using facial recognition. Computers will make real-time judgments about the person being identified. So, what happens if one is incorrectly identified as a terrorists or criminal?

Since facial recognition can be used for enrollment and surveillance without the individual's knowledge, it was no surprise that ICAO and its stakeholders (June 28, 2002) unanimously endorsed the "*Berlin Resolution"* for "*the use of facial recognition as the globally interoperable biometric for machine assisted identity confirmation with MRTD's (machine readable travel documents)"*[xvii]

FACIAL RECOGNITION TESTS

Facial recognition is being promoted as a tool against terrorism. But, will facial recognition make us safer? Facial recognition failures are highly documented[xviii] even in AAMVA's 2003 "International Biometric Group" (IBG) report[xix] the following was concluded regarding its use.

- POOR performance
- Grossly exaggerated vendor claims
- Facial recognition will not perform successfully in a large database of 300 million
- Real world tests at Colorado's DMV revealed only about 1% accuracy
- Facial recognition has difficulty with glasses and facial hair

The DHS sponsored, Facial Recognition Vendor Test 2006 (FRVT 2006)[xx] also reflected inflated vendor estimates, prompting biometrics expert, Ben Bavarian to state that the tests are *"only valid for the defined*

circumstances of the NIST ITL labs" and these tests are "*turned into marketing tools for vendors to push the products without doing the right things for the technology."*

HIGH-TECH TOOLS–Human Dignity, Civil Rights, Testing, Function and Security are Secondary

Like facial recognition, DHS shares equal disregard for other testing procedures. On September 18, 2007, the Washington Post reported,[xxi] that weeks before key government tests of new radiation detection equipment, DHS officials "helped" contractors through repeated dry runs that enabled them to perform better during the examinations. Congress expected to use the long-awaited tests to make a $1.2 billion decision. Congress was previously concerned that DHS misled them about the device's effectiveness, known as Advanced Spectroscopic Portals, or ASPs.

Instead of investing in "real" security, DHS spent millions on Boeing's "virtual fence," that did not work.[xxii] DHS is also testing the "virtual strip search," machine, AKA-backscatter device, recently deployed in Phoenix.[xxiii] Another new item being tested is "Project Hostile Intent"[xxiv] that will "*identify*" terrorists' *"intent*" by judging behavior and facial expressions.

POWER, CONTROL, DECEIT AND FAILURE

Consider the numerous technology failures, the deceit of government agencies and the constitutional risks. How can we trust biometrics, biometric vendors, international organizations and government agencies employing biometrics? REAL ID grants DHS almost unlimited powers. DHS can also redefine their powers as they see fit. NPRM states that the "official purpose" of REAL ID: ``***includes but is not limited to accessing Federal facilities, boarding Federally-regulated commercial aircraft, entering nuclear power plants, and <u>any other purposes that the Secretary shall determine</u>.***'' The section goes on to say, *"...**under the <u>discretionary authority</u> granted to the Secretary of Homeland Security under the Act, may <u>expand</u> this definition in the future.**"* Even REAL ID "final rules" are not "final" being full of "potential changes."

- Global biometric ID and database linking threaten religious rights, privacy, states' rights, and our sovereignty, creating a global system of financial control, linked to our bodies, run by international organizations. The most powerful document we possess will be out of our control. Potentially, REAL ID requirements could be imposed on banking, Medicare or cashing Social Security checks, school ID, etc. or any form of identification relating to a federal agency.

- Database linking-sharing will certainly result in an ID theft pandemic. The consolidation of power in one document increases the chances of ID fraud just as data sharing increases the risk of ID theft.

- Facial recognition will NOT work effectively on terrorists unless they submit to enrollment and *shave*.

- Other countries will issue biometric ID based on their own "breeder" documents (ex. birth certificate). Based on those "breeder" documents, e-passports will be accepted at face value. Persons issuing foreign e-Passports, must be experts in identifying fraudulent "breeder" documents or the biometric ID permanently legitimizes the fraud.

- This system places our national security on the shoulders of government employees in other countries.

- Every government to which we link databases, must have secure "records" buildings, information technology systems and totally trustworthy employees protecting highly personal information collected globally (shared databases). DHS-TSA lost a hard drive with thousands and thousands of employee

records. Great Britain recently lost two disks containing personal information of 25 MILLION people, half the country. How will DHS secure ID systems of other nations? If a nation builds financial systems on biometrics and the biometrics are compromised, the entire system becomes useless.

- DHS has difficulties with information sharing between all levels of law enforcement. DHS plans to expose highly personal information of U.S. citizens, doesn't mean other nations will provide the U.S. with accurate, and highly personal information, on all their citizens.

REAL ID, Western Hemisphere Travel Initiative (WHTI), e-passport, Transportation Worker Identification Credential (TWIC), backscatter, virtual fence, "Project Hostile Intent" etc. are indicators of the current DHS mindset that **can't keep its hands out of the technological cookie jar**. While technical failures mount, our nation becomes less secure. DHS is wasting billions of dollars on "high-tech" failures instead of investing in fences and people desperately needed on our borders and in our ports. This "DHS mindset" has not escaped the notice of the Government Accounting Office (GAO), that cited many problems with DHS, giving it a several failing grades.

FREEDOM WILL PREVAIL

Solutions are found in the freedoms being destroyed. We must stand up for our rights. DHS plans rely on the public being uninformed and the use of deceit, not transparency. Therefore educate, legislate and be willing to work with others of different political affiliation. Biometrics is NOT about political parties!

PROPOSED LEGISLATION -- TAKE ACTION

Stopping REAL ID is not enough – DHS will impose biometrics, global data sharing, and collection of personal information through REAL ID, other legislation or through L1's "monopoly" of state DL/ID cards. Once state databases are "standardized," DHS can legally access state records and share personal-biometric information globally. Standardization must occur before sharing, so the goal of state legislation is to make state databases UNUSABLE for sharing, incomplete, incompatible with facial recognition, etc. **Use this document to inform state and U.S. lawmakers of the problems and solutions (below). Email "Stop REAL ID Coalition" for digital copies of documents and proposed legislative text. Share this document with lawmakers and ask them to author or support legislation that will:**

- Ban participation in REAL ID
- Ban the use of biometrics, reduce DL/ID card photo resolution so it is incompatible with facial recognition and wipe existing biometric data
- End the collection and storage of Social Security Numbers and end state participation in federal programs that collect a SSN (through DL/ID cards) and share data through AAMVA
- Require the Legislature and Governor to approve ALL DL/ID card related rules and information sharing agreements, by state motor vehicle departments, before implementation (for transparency - no hidden biometrics, AAMVA, ICAO, etc.)
- Establish a state-to-state data sharing system and do away with AAMVA sharing for non-Commercial Driver Licenses

Below is a more detailed list of propose legislation with the more important issues highlighted.

BAN REAL ID

- **Ban state participation in REAL ID or any federal law that mandates federal or international standards for state ID (As of July, 2008 many states have already passed such legislation)**

IMPROVE ID DOCUMENT INTEGRITY

- Encourage federal legislation that funds states' efforts to improve ID document integrity, rather than punish for non-compliance. But, biometrics or photo standards must not be included in the "improvements."

MAKE CURRENT STATE PHOTOS/DATABASES UNUSABLE WITH FACIAL RECOGNITION AND GLOBAL INFORMATION SHARING–WIPE BIOMETRIC DATA

- **Photo resolution must not exceed 24 pixels between eye centers for all DL/ID cards and CDL cards. This level of resolution makes photos suitable for printing and human recognition, but is far below the resolution required for facial recognition (ICAO currently requires 90 pixels between eye centers). Lower cost since no facial recognition software is needed, low-resolution cameras will be sufficient**

- **No biometrics – ban the use of all biometrics for all DL/ID cards and CDL cards.**

- Seek to recollect all previously shared biometric data or high-resolution photos.

- **Ban the use of any DL/ID vendor's biometric software (ex. Viisage's FaceEXPLORER) upon passage of any law banning facial recognition. These software programs must be "turned off" or uninstalled from ALL computers.**

- Provide OPT-OUTS for state retention of photo (non-CDL)– State will issue the DL/ID, print the DL/ID card and wipe photo from state records. This makes the state database incomplete, unsuitable for sharing.

- **Wipe state DL/ID card databases of all existing high resolution photos and fingerprints (if applicable)**
- **Wipe all biometric information, including high-resolution photos, from all of state "backup" systems**
  NOTE: Existing biometric data must be wiped using PERMANENT data wiping algorithms
  NOTE: Because of DL/ID vendor issues, contract cycles, etc. Legislators may need to work with agencies to accomplish the goals so that legislation is not increasing expense unnecessarily. In many cases, biometric software can be "turned off" without completely changing DL/ID card vendor's software or renegotiating a vendor contract. Turning off software would cost nothing. Photo resolution can often be reduced through software switches even using high-resolution cameras. The camera controls the maximum resolution that can be collected, but software controls actual photo resolution.

- Extend the DL/ID renewal cycle to 6-8 years. With previously stated changes and longer renewals, re-enrollment into another "REAL ID-like" system will take much longer.

- Consider 3rd party supervision (state "IT" specialists) to ensure state agency compliance with new laws.

- Ban scanning and storage of "breeder documents" used for initial DL/ID application (ex. birth certificates).

PROTECT PERSONAL INFORMATION FROM STATES, AAMVA and FEDERAL AGENCY ACCESS

- **No SSN collected for DL/ID (CDL – N/A) – Defy the Child Welfare Protection Act requirements for SSN collection. A few states do not collect a SSN and are not penalized by the federal government, according to a recent GAO report. Penalties cannot be imposed since the law is inherently illegal. State DL/ID cards must not be used for compliance with any federal program or law.**

- **No Selective Service election (information, including SSN's are shared through AAMVAnet) – young men 18-26 are required by federal law to register with Selected Service anyway.**

- **No voter registration through DL/ID application (personal information shared through AAMVA)**

- **Allow mailing addresses on DL/ID cards - protect privacy**

- OPT-OUTS for state retention of SSN (if state chooses to collect SSN). Persons can choose to Opt-Out of state retention of SSN. If state verifies SSN, verification must be with SSA only – not through AAMVA. No document or computer record (with a SSN) is to be kept by state – shred all documents with SSN.

- **Ban the sale of personal information collected by all state agencies**

- Immigration laws must not require the use of E-Verify since information is funneled through AAMVA or DHS control and access – identification can be verified directly with appropriate agency

- Ban the "retail swiping" of barcodes or magnetic strips, on DL/ID cards – used to collect personal information

- Ban participation in AAMVAnet and any AAMVA compact or agreement regarding NON-Commercial driver's licenses (non-CDL). Non-CDL data should be shared directly with other states (not through AAMVA). Allow 2-3 years for implementation and reciprocity agreements to be formed between states, with the goal of sharing information directly and under the control and watchful eye of State Legislators. Promote NGA and NCSL participation in new system. Businesses create secure Internet sharing systems everyday. There is no reason to keep AAMVAnet. However, by retaining membership in AAMVA and sharing CDL information through AAMVA, states can keep federal funds relating to CDL-Highway issues, but only a state-to-state system will protect personal information of those with non-CDL licenses and ID cards.

- Motor vehicle/law enforcement officials must be prevented from communicating with AAMVA regarding the use of biometrics or other technologies once a new DL/ID card law is passed

CONTROL GOVERNMENT AGENCIES UNDER STATE JURISDICTION

- **Regarding the identification and personal information sharing of individuals, no state agency shall enter into agreements, contracts, compacts or create rules, or generally supply such information, to federal agencies organizations, businesses or other government entities unless such agreements, contracts, compacts and rules are first approved by the State Legislature and the Governor.**

- **Regarding the identification and personal information sharing of individuals, no state agency shall implement rules regarding such laws, unless the Legislature and the Governor have approved those rules.**

- Require state agencies to account for ALL time and expenses spent "lobbying" for or against any legislation.

- Ban use of biometrics for all government agencies, municipalities, schools, etc. (except for criminal records), under state jurisdiction, including the use of biometric time clocks for government employees, preventing cities from using or partnering with DHS for facial recognition surveillance, etc. NOTE: It will be almost impossible to remove biometric fingerprinting from criminal and penal records. But, a procedure must be in place to remove any biometrics of a person proven to be innocent of a crime.

- **B**an the remote collection of biometrics (Traffic officers collecting facial images, fingerprints, etc.).

- Readable signs must be posted near public surveillance cameras (ex. intersection or highway surveillance) indicating what agency is responsible for the camera, the purpose of surveillance and contact information regarding the camera's use. Many municipalities are receiving grant money from DHS for public surveillance.

- **Require that government documents requesting a SSN state if the collection of the number is mandatory or voluntary. If mandatory, the law mandating its use must be listed.**

- **Ban collection of SSN for public documents (ex. professional license, marriage license, etc.)**

BUSINESS-PRIVATE USES OF BIOMETRICS - PROTECTION OF PERSONAL INFORMATION

- 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, thus 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 – Such restrictions will help limit government data mining.

- Require insurance companies to REMOVE Social Security numbers from their records.

- Require insurance information services (ex. ISO - Insurance Services Office, Inc.) to remove SSN information from their records for state residents and to prevent the use of "auto-fill" to automatically add a SSN, gathered from other sources, to personal records. An individual may refuse to supply a SSN to an insurance company or medical practitioner. "Auto-fill" can be used to ADD the SSN (collected from other sources) to the individual's records without their knowledge or approval.

- Require private sector and public services, like hospitals, that collect biometric data, to notify individuals of the use of biometrics and to provide an alternative form of ID – (ex. birth records, employee ID, etc.).

- Require businesses that use biometrics in surveillance to post public notification (ex. Las Vegas hotels – Casinos, etc.).

- Require that businesses requesting a SSN, state if the collection of the number is mandatory or voluntary. If mandatory, the law mandating its use must be listed.

- Defy portions of the PATRIOT ACT and other federal legislation that mandates the collection of a SSN for non-interest bearing bank accounts.

- Prevents banks from denying service for refusing to provide a fingerprint or a biometric identifier.

SUGGESTIONS FOR SUCCESS

- BI-PARTISAN SUPPORT - Get bi-partisan support, authors and co-authors from both parties

- COMMITTEES - Get to the heads of committees for authorship and support. Be prepared to face off with DMV officials about the accuracy and constitutionality of biometrics and information sharing.

- COST – Legislation should include a cost analysis to avoid an excessively high cost supplied by an opposing agency - Some costs can be reduced simply by turning off DL/ID vendor functions (facial recognition) and changing photo resolution through software switches, rather than forcing a complete renegotiation of a vendor contract. However, many state DL/ID-vendor contracts have provisions for accommodating changes in law.

- CONTRACT – Get a copy of the DL/ID vendor contract, ALL "Request for Proposal" or "Request for Information" documents, especially those indicating expected accuracy with facial recognition.

- Begin the session with multiple bills, that are germane, yet worded differently so that one bill can be amended with "similar" wording from a bill that is killed in committee (ex. pixels between eye centers or total pixels for head width, image height and width, etc.).

- FACIAL RECOGNITION FAILURES - Gather information from DL/ID card issuing agencies about the REAL successes (failures) of facial recognition, including total cost, total convictions relating to driver's license fraud, total criminal court cases and convictions directly attributed to facial recognition or DL/ID fingerprinting (if applicable) or collection of SSN's. Force the DMV to justify the cost and reconcile the benefits against the civil rights issues. Total number of "facial image matches" compared to ACTUAL matches, daily, weekly, yearly – How many false matches compared to real matches? - Proves inaccuracy and how much time is wasted weeding out false matches. Note any breaches in security to the DMV system – hacker attacks per day.

- EDUCATE – EDUCATE - EDUCATE – Pass out documentation to committee members first, then members of both Houses and the Governor. Idaho's REAL ID legislation was a direct result of this tactic. The uniformed supporters of REAL ID or biometrics may become allies when given the facts.

The mission of the Stop REAL ID Coalition is to STOP REAL ID, STOP the use of biometrics in ID documents, STOP unconstitutional information sharing and STOP the influence of international organizations on state and federal law. These threats touch EVERY American. So, the Coalition has worked hard with both conservative and liberal lawmakers, groups and individuals in DC and in many states. The Coalition has provided evidence to officials with the U.S. House Homeland Security Committee and the U.S. Finance Committee. We have also obtained similar letters of opposition, to these threats, from the most conservative and most liberal legal authorities in the nation, the American Center for Law and Justice (ACLJ) and the American Civil Liberties Union (ACLU). For more information email us stoprealid@aol.com. Email "Stop REAL ID Coalition" for digital copies of documents and proposed legislative text.

REFERENCE PAGE

[i] Source GCN –DHS pushes global data sharing – http://www.gcn.com/print/26_03/43061-1.html
[ii] Source AAMVA – "Current and Ongoing Efforts – http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm

[iii] Source ICAO – Tag/Mrtd17_WP016.pdf (Jan. 2007) "Background 2.1"

[iv] Source AAMVA web site – www.aamva.org and listed on other source documents (see note i – Current and Ongoing Efforts – http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm)

[v] Source AAMVA - http://www.aamva.org/KnowledgeCenter/Driver/Compacts/History+of+the+DLA.htm

[vi] Source AAMVA – std2005DL-IDCardSpecV2FINAL.pdf

[vii] Source H.R.418 REAL ID ACT of 2005 – Sec. 203 "Linking of Databases" – re: "Driver License Agreement" //NOTE: HR418 from House was included in HR1268 in Senate, passed and signed into law

[viii] Source DHS – "Notice of Proposed Rulemaking" (Mar. 1st 2007), "H. Minimum Driver's license or identification card Data Element Requirements - Sec. 5 Signature, Sec. 8. Machine Readable Technology (MRT) barcode standard, data elements, Sec. 9 Encryption (barcode) J. Source Document Retention (and related sections detailing these requirements) - nprm_readid.pdf --- Note: The **"Privacy Impact Assessment for REAL ID ACT"** is cited in the document and was issued with the NPRM --- REAL ID Final Rules issued January 11th, 2008.

[ix] ICAO announces (July 11th 2005) the Machine Readable Passport (MRP) standard specified by ICAO is the international standard – pio200507_e.pdf

[x] "Enhanced Border Security and Visa Entry Reform Act of 2002" "Sec. 303 Machine Readable Tamper Resistant Entry and Exit" requires biometric Machine Readable Passports, complying to ICAO standards, for "visa waiver nations."

[xi] Source ICAO – Tag/Mrtd17_WP016.pdf (Jan. 2007) 3.1 Creation of ICAO

[xii] Source ICAO – Tag/Mrtd17_WP20.pdf (March 12th, 2007) "2. ONGOING WORK OF THE NTWG SINCE TAG/16" sec. 2.2

[xiii] Source DHS – (See ref. iii) - The ISO/IEC 19794-5 standard defines how photos, compatible with facial recognition biometrics, are to be collected when used in ICAO's 9303 Machine Readable Travel Documents (MRTD).

[xiv] Source DHS – http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm

[xv] Source DHS – "Notice of Proposed Rulemaking" (Mar. 2007) – section 3 "Digital Photograph" (March 2007) footnote (17) states "*The relevant ICAO standard is ICAO 9303 Part 1 Vol 2, specifically ISO/IEC 19794-5 - Information technology - Biometric data interchange formats - Part 5: Face image data, which is incorporated into ICAO 9303*" nprm_readid.pdf

[xvi] Source Wall Street Journal Article July 8th, 2005 "Surveillance Cameras Monitor Much of Daily Life in London May Help to Identify Bombers" - http://online.wsj.com/public/article/SB112077340647880052-cKyZgAb0T3asU4UDFVNPWrOAqCY_20060708.html

[xvii] Source ICAO – TagMrtd17_WP016.pdf – 5.3 SELECTION OF BIOMETRICS MODALITIES FOR E-PASSPORTS

[xviii] Source Washington Technology – Great Expectations – Biometrics – http://www.washingtontechnology.com/print/18_13/21791-2.html

[xix] Source AAMVA IBG Report - UID9BiometricReport_Phase1_1to300m.pdf

[xx] Source FRVT2006andICE2006LargeScaleReport (4).pdf http://frvt.org/FRVT2006/default.aspx

[xxi] Source Washington Post (Sept. 18th 2007) "DHS 'Dry Run' Support Cited" http://www.washingtonpost.com/wp-dyn/content/article/2007/09/17/AR2007091701718.html?hpid=moreheadlines

[xxii] Source AP "Glitch Renders 'Virtual Fence' Unusable (Sept. 20th 2007) – http://www.washingtonpost.com/wp-dyn/content/article/2007/09/19/AR2007091902664.html

[xxiii] Source USA Today - Phoenix test site for TSA X-ray -http://www.usatoday.com/printedition/news/20061201/1a_lede01art.htm

[xxiv] Source DHS- Deception Detection: Identifying hostile intent – http://www.homelandsecurity.org/snapshots/newsletter/2007-05.htm#deception

A Brief List of Laws, Initiatives and Treaties Relating to a Global Biometric ID System

- The "**Commercial Motor Vehicle Safety Act of 1986**" attempted to impose biometrics on state ID for identifying commercial driver's license holders

- **1995 ICAO** began work on biometric Machine Readable Travel Documents (MRTD's) resulting in ICAO 9303 TAG-MRTD/17-WP/16.pdf (1-6-07)

- The "**Illegal Immigration Reform and Immigrant Responsibility Act of 1996**" set federal standards for all driver's license/ID cards (DL/ID cards) and placed state DL/ID card design under the influence of AAMVA

- **"Enhanced Security and Visa Reform Act of 2002**" – biometrics collected on visa holders - Visa Waiver nations issue biometric passports designed by ICAO

- **REAL ID ACT of 2005** and **NPRM** require states to:
  1. Collect, store and share highly personal information verified through online systems (ex. DHS "federated querying" system or AAMVAnet)
  2. Adopt global biometric DL/ID card standards set by AAMVA and ICAO "9303" photo standards complying with "**biometric data interchange formats**" making all photos compatible with facial recognition software
  3. Link state DL/ID databases, creating common database systems (DLA model) – Once databases link, the photos can be accessed by government agencies outside the state. The images can then be used with common facial recognition systems. State database linking and information sharing permanently enrolls U.S. citizens in a global biometric system. Data cannot be retrieved once distributed. The shared data can then be shared globally as part of an international database linking system.

- **Initiatives – WHTI** (Western Hemisphere Travel Initiative) requires a passport for travel between Canada, United States and Mexico as of 2007– WHTI meant new applicants issued new biometric e-passports (ICAO design). DHS began pilot program with Washington, Arizona and New York to issue biometric DL/ID card/passport hybrid acceptable as passport. **TWIC** (Transportation Worker Identification Credential) - Requires biometric ID cards for thousands of government employees

- **July 2007, the EU and US begin sharing new database information** on travelers, including "*racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership" and "data about an individual's health, traveling partners and sexual orientation"* according to a July 27th, 2007 Washington Post article. Such data collection and sharing depends on other federal laws, like the recently revised FISA, to permit surveillance and data mining of information on U.S. citizens. Robert Mocny (DHS-US Visit) stated that global data sharing would begin with Europe, Asia (GCN February 5th, 2007).