

REAL ID-BIOMETRIC FACT SHEET

Final Rules

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

The REAL ID ACT of 2005 does not create a national ID card but an INTERnational BIOMETRIC ID card

The world is being enrolled into a single global biometric ID system through driver's license/ID cards (DL/ID cards), passports and other ID documents. Biometrics, like facial recognition, digital fingerprinting and iris recognition, are already being used by many states and nations. The federal government attempted to impose biometrics on state ID in 1986ⁱ. International biometric plans were laid in 1995ⁱⁱ. Both predate 9/11. The biometrics required by REAL ID, other security laws, initiatives, treaties and agreements, are not needed tools against terrorism, but the fulfillment of a global biometric ID system.

On March 1st, 2007 REAL ID's "Notice of Proposed Rulemaking" (NPRM) was issued, revealing REAL ID's global biometric connectionⁱⁱⁱ. The three main entities driving this system are:

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

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, DLA and other document standards are requirements, cited in REAL ID HR418^{vii} and/or NPRM^{viii}. AAMVA's influence over international, federal and state DL/ID card laws is evident in REAL ID (mentioned 30 times in NPRM and 150 times in REAL ID final rules 01-11-08)^{viii}.



ICAO monitors travelers, designed biometric "e-passports^{ix}" required for "Visa Waiver Nations^x" and is affiliated with the UN^{xi}. Global enrollment into the e-passport system is 50 million annually^{xii}. REAL ID photos comply with ICAO "**biometric data interchange formats**"^{xiii} standards, making state photos compatible with global biometric facial recognition standards.

Together, DHS, AAMVA and ICAO are fulfilling the three elements necessary for a global biometric system.

1. Common "interoperable" document and biometric standards set by ICAO-AAMVA
2. Biometric enrollment (passports, DL/ID cards, military ID, government employee ID, birth records, etc.)
3. International database linking containing personal-biometric information (DHS-AAMA-ICAO)

REAL ID and NPRM and/or REAL ID final rules, require states to:

1. Adopt biometric photo standards set in ICAO 9303^{xiv}, a minimum resolution of 90 pixels between eye centers
2. To verify identification "breeder" documents and supporting documents through an online system (proposed systems include DHS sponsored "federated querying"^{xv} and AAMVAnet^{xvi})
3. Adopt documentation standards set by AAMVA
4. Link state databases and participate in AAMVA's DLA

After issuing the NPRM, DHS released "20 Questions and Answers"^{xvii} 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 INTERnational ID. DHS can "legally" access database information through the outdated "Drivers Privacy Protection Act" (DPPA) and the DHS proposed "federated querying system" or AAMVAnet (described in the Final Rules as the "backbone" of the system). REAL ID DOES require photos

compatible with facial recognition biometrics and any government agency accessing the linked database system can use any state photo with facial recognition software, making it a biometric.

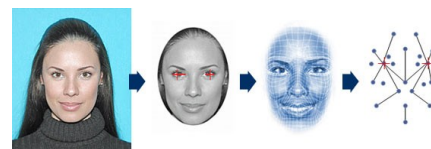
DHS denies that REAL ID requires biometrics but the “**Privacy Impact Assessment for REAL ID ACT**” (March 1, 2007) clearly states; “*In addition, as a result of the Act, state databases will contain **standardized photo images that will allow law enforcement agencies to use facial-recognition technology 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)

REAL ID standards make state databases “interoperable” and database linking will result in states losing control of their ID system. The DL/ID card controls our ability to buy, sell and move. While under state control, this power remains under the control of the people who have access to the lawmakers administering its use. REAL ID places that control under federal and international entities through laws, initiatives and treaties, some of which are listed below.

FACIAL RECOGNITION – The Global Biometric of Choice

Facial recognition creates a digital, machine readable, map of one’s face. 3-D facial recognition potentially identifies individuals in “real world” settings, addressing issues of lighting and movement, providing the tool for a surveillance society like Great Britain with an estimated 500,000 surveillance cameras in London and 7 million nationally.^{xviii}

On June 28, 2002, the ICAO, and its stakeholders, 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)*”^{xix} **Why Facial Recognition?**



Facial recognition can use existing digital photo databases (enrollment) and is suitable for public surveillance.

FACIAL RECOGNITION TESTS –

National security funds are wasted on biometrics. Facial recognition failures are highly documented^{xx} even in AAMVA’s 2003 “International Biometric Group” (IBG) report^{xxi}. The report “anticipates” (by two years), the linked database requirements of REAL ID (300 million drivers), demonstrating AAMVA’s influence on federal legislation.

The IBG report reveals:

- “Synopsis of facial image recognition performance is **POOR.**”
- Test results on a “**100-person database**” showed “**only “53% of multiple enrollees were identified correctly”** and “*The comparatively small size of this database, and the error rates encountered, call into question the scalability of facial recognition for much larger systems*”(pg 10).
- “...facial recognition will **not be capable** of successfully performing 1:300m (million) identification”(pg 17).
- IBG evaluated a Colorado DMV case study using facial recognition to look for duplicate DL/ID cardholders. On 3000 applicants/day, the facial recognition program produced 100-125 facial image matches/day. “**False Matches**” were **99%** of those, making **only 1% valid** (about 1 per day or 26 per month (pages 93-94).
- Facial recognition has great difficulty with facial hair and glasses (pages 30-32, 117).
- “**Vendor’s performance projections**” - “**Estimated 69% correct ID rate on 300m** (million) database” (pg 16). Vendor claims for a 1:300 million environment, exceed the small 100-person database test result (53%)!

The DHS sponsored, Facial Recognition Vendor Test 2006 (FRVT 2006)^{xxii} 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.*”

DHS WANTS MORE HIGH-TECH TOOLS–Human Dignity, Civil Rights, Testing & Function are Secondary

Like facial recognition, DHS shares equal disregard for other testing procedures. On September 18, 2007, the Washington Post reported,^{xxiii} 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 doesn't work.^{xxiv} DHS is also testing the "virtual strip search," machine, AKA-backscatter device, recently deployed in Phoenix.^{xxv} Another new item being tested is "Project Hostile Intent"^{xxvi} that will "identify" terrorists' "intent" by judging behavior and facial expressions. The suspicious test procedures and failed tests by DHS-TSA are too numerous to mention in this document.

POWER, CONTROL AND DECEIT

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 any other purposes that the Secretary shall determine.*" The section goes on to say, "*...under the discretionary authority granted to the Secretary of Homeland Security under the Act, may expand this definition in the future.*" Even "final rules" is full of "potential changes."

REAL ID's official purposes have already changed to discourage further opposition i.e. access to national parks. Potentially, REAL ID requirements could be imposed on banking, Medicare or cashing Social Security checks, school ID, etc. **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.**

DL/ID Card Photo = Biometrics and deceitful enrollment. Why use facial recognition? Enrollment. The 2003 IBG report states, "*Facial recognition technology can acquire faces from almost any static camera or video,*" and "*Facial recognition databases...are capable of creating databases from facial images not specifically collected for biometric usage.*" Linked databases with photos = facial recognition database.

RUSHING TO FAILURE – Increasing Risk and Wasting Resources

Robert Moczny (DHS 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.*"^{xxvii} DHS is committed to global data sharing and is "rushing" to fulfill a global biometric dream, before November 2008. Risking it all, DHS ignores the facts about, global biometrics, data sharing, allowing international organizations to influence U.S. law and REAL ID.

- 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.
- 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, those documents, 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 Peru, Columbia, Haiti, Bolivia, Pakistan, Saudi Arabia, China, etc.
- Every government 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?
- DHS has difficulties with information sharing between all levels of law enforcement. How can we rely on other nations to share 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 recently cited many problems with DHS, giving it a several failing grades.

REAL ID and other biometric laws must be repealed. States must take back power from international organizations, wipe databases of biometrics and biometric compatible information, and reduce the quality of photos, making them unusable for biometrics (max. 25 pixels between eye centers), protecting state databases from future takeovers.

012208 REAL ID –BIOMETRIC FACT SHEET-final rules.doc

REFERENCE PAGE

- ⁱ Source AAMVA – “Current and Ongoing Efforts – <http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm>
- ⁱⁱ Source ICAO – Tag/Mrtd17_WP016.pdf (Jan. 2007) “Background 2.1”
- ⁱⁱⁱ 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
- ^{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} ICAO 9303 - ISO/IEC 19794-5 is available from ISO (see 040607 April_6_FP_Published_ISO_Standards.pdf), however, “Annex D-Face Image Data Interchange.pdf” addresses similar content and can be downloaded.
- ^{xv} Source DHS – “Notice of Proposed Rulemaking” (Mar. 1st 2007), “Sec. 6. a, ii. Federated Querying Service - nprm_readid.pdf
- ^{xvi} Source DHS - Privacy Impact Assessment for the REAL ID ACT of 2005- Sec. 3 “The State to State Data Exchange” (footnote 24) refers to AAMVAnet as one part of a current data exchange program that could be used

to implement the requirements of REAL ID's database linking requirements – privacy_pia_realid.pdf. Source DHS REAL ID Final Rules, refers to AAMVAnet as the “backbone” of this data sharing system.^{viii}

^{xvii} Source DHS – http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm

^{xviii} 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

^{xix} Source ICAO – TagMrtd17_WP016.pdf – 5.3 SELECTION OF BIOMETRICS MODALITIES FOR E-PASSPORTS

^{xx} Source Washington Technology – Great Expectations – Biometrics – http://www.washingtontechnology.com/print/18_13/21791-2.html

^{xxi} Source AAMVA IBG Report - UID9BiometricReport_Phase1_1to300m.pdf

^{xxii} Source FRVT2006andICE2006LargeScaleReport (4).pdf <http://frvt.org/FRVT2006/default.aspx>

^{xxiii} 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>

^{xxiv} Source AP “Glitch Renders ‘Virtual Fence’ Unusable (Sept. 20th 2007) – <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/19/AR2007091902664.html>

^{xxv} Source USA Today - Phoenix test site for TSA X-ray
-http://www.usatoday.com/printedition/news/20061201/1a_lede01.art.htm

^{xxvi} Source DHS- Deception Detection: Identifying hostile intent – <http://www.homelandsecurity.org/snapshots/newsletter/2007-05.htm#deception>

^{xxvii} Source GCN –DHS pushes global data sharing – http://www.gcn.com/print/26_03/43061-1.html

A brief list of laws, initiatives and treaties being used to impose 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 Moczynski (DHS-US Visit) stated that global data sharing would begin with Europe, Asia (GCN February 5th, 2007).