

REAL ID-BIOMETRIC FACT SHEET

The Final Chapter in a Systematic Plan for Global Biometric ID

Submitted by STOP REAL ID – an association of concerned citizens

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

The world is being enrolled in an international biometric ID system through driver's license/ID cards (DL/ID cards), passports and other ID documents. 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 a (DMV-DPS) data linking system, 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} The 2005 DL/ID standard, DLA and various other document standards are requirements, cited in REAL ID^{vii} and NPRM^{viii}. AAMVA exercises great influence over international, federal and state level DL/ID card laws, evident in REAL ID (AAMVA is mentioned 30 times in NPRM).



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 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

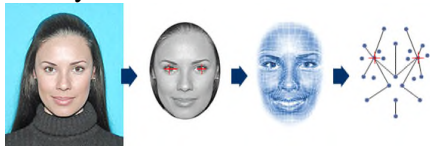
REAL ID is an INTERnational ID. DHS can "legally" access database information through the outdated "Drivers Privacy Protection Act" (DPPA) and the DHS proposed "federated querying system." REAL ID DOES require photos

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.

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:

- 1 “Synopsis of facial image recognition performance is **POOR.**”
- 2 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).
- 3 “...facial recognition will **not be capable** of successfully performing 1:300m (million) identification”(pg 17).
- 4 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).
- 5 Facial recognition has great difficulty with facial hair and glasses (pages 30-32, 117).
- 6 “**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 suspect 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.*”

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.

- 1 Global biometric ID and database linking threaten religious rights, privacy, states’ rights, and our sovereignty.
- 2 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.
- 3 Facial recognition will NOT work effectively on terrorists unless they submit to enrollment and *shave*.
- 4 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.
- 5 This system places our national security on the shoulders of government employees in Peru, Columbia, Haiti, Bolivia, Pakistan, Saudi Arabia, China, etc.
- 6 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. How will they secure ID systems of other nations?
- 7 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.

093007 REAL ID -BIOMETRIC FACT SHEET.doc

A CHRISTIAN PERSPECTIVE on REAL ID and BIOMETRICS

This document is an attachment to "REAL ID-BIOMETRIC FACT SHEET"

Submitted by STOP REAL ID -an association of concerned citizens

THE THREAT

The REAL ID ACT of 2005 has provoked opposition from all aspects of our society. New Hampshire's ban of REAL ID called it "repugnant." Many conservative Christians oppose REAL ID for religious reasons. Other groups, like the ACLU, oppose REAL ID but for reasons of privacy. Opposition to REAL ID is more like a war, where differences are thrust aside because of a common enemy. For example, REAL ID requires digital photographs (compatible with biometric facial recognition). Therefore it violates the religious beliefs of some smaller Christian denominations, like Mennonites, but it also violates the religious rights of many Muslim women. The issue is protecting freedom for all. This concept was not wasted on Corrie ten Boom or Dietrich Bonhoeffer, the great German theologian of WWII, who died preserving such freedoms.

REAL ID also threatens the beliefs of mainstream, conservative, evangelical Christians. Biometrics and database linking create an international system of financial control linked to one's body similar to the mark of the beast described in the Book of Revelation. Biometrics is an international ID system with standards, set by international organizations. The purpose of these standards is to create a platform for sharing personal-biometric data globally. Global data sharing is not possible unless nations and states link databases (required by REAL ID). The Department of Homeland Security (DHS) has made it very clear that personal-biometric information, collected by nations and corporations, will be shared globally. Similar to Revelation 13:16, this global ID system would apply to "all" just like the mark of the beast.

Rev 13:16-17

16 And he causes all, the small and the great, and the rich and the poor, and the free men and the slaves, to be given a mark on their right hand, or on their forehead,

17 and he provides that no one should be able to buy or to sell, except the one who has the mark, either the name of the beast or the number of his name.

(NAS)

Biometrics and global data sharing create a system of financial control linked to one's body similar to Revelation 13:16-17. This is accomplished in two main ways.

1. Allowing and preventing financial transactions based on biometric enrollment and possession of biometric ID

The current “official purposes” of REAL ID would prevent the use of a non-compliant driver’s license/ID card (DL/ID card) for flying commercially, entering federal buildings or entering nuclear power plants. More recently, DHS added national parks to that list. However, DHS powers are not limited to those purposes. REAL ID requirements can apply for *“any other purposes that the Secretary shall determine.”* and that DHS *“may expand this definition in the future.”* Potentially, only a REAL ID - DL/ID card could be used for banking, cashing Social Security checks, Medicare, etc. Before the 2007 “Immigration Bill” was stopped, biometric Social Security cards were proposed, and employment would be contingent upon possession of a REAL ID card. In other words, the trend is NO BIOMETRICS = NO buying, selling and driving or flying. Of course, one could use a passport for official federal purposes, but they are biometric now as well.

2. Using biometrics for identification in the completion of a financial transaction

In 1996, AAMVA proposed a universal biometric DL/ID Smart Card, replacing ALL other ID and financial documents. A microchip would store biometric and personal information (much like the new e-passport today). ID would be verified before by a hand or facial scan. More recently VISA-USA began testing a “fingerprint” credit system (no plastic). Since 1996, there have been, literally thousands of financial uses for biometrics.

IS THIS THE ENROLLMENT FOR THE MARK OF THE BEAST?

The current biometric ID system is not the mark of the beast, but would easily qualify as the enrollment process for it. Imagine, a linked database system, containing the personal and biometric information of almost every person in the world, accessible from almost anywhere in the world. This is the disturbing “vision” of DHS and, unfortunately, it is happening at a staggering rate. The ICAO estimates global enrollment into the biometric e-passport system to be 50 million annually.

THE MARK?

For years many have speculated that the mark may be a microchip. Recently a company called Somark (St. Louis, MO) developed ink RFID “tattoos” that works like a standard RFID chip. RFID chips store and transmit information just like a “Turnpike Pass”. A signal is transmitted that activates the RFID chip. The chip then transmits its stored information. ID information is stored in the “digital ink” RFID “mark” or “tattoo” imbedded in the skin and is currently being targeted for cattle, industrial and military applications. Technologies like the RFID tattoo may provide clues as to what the “mark” of Revelation 13 might be.

PERMANENT ENROLLMENT

Biometric enrollment could occur simply through database linking (required by REAL ID). Existing digital photos, in DL/ID databases, could be used for biometric facial image recognition. Linked with other personal information, data could be shared globally even without one’s knowledge. This is why ICAO and DHS elected to use facial image recognition as the biometric of choice for global data sharing. Also, facial recognition is suitable for public surveillance, identification and tracking.

DHS engaged in wishful thinking when deploying facial recognition biometrics. The tests available at the time current laws and initiatives were written, proved the ineffectiveness of facial recognition. Yet, DHS pushed this technology on U.S. citizens, spending millions and millions on an almost worthless tool against terrorists. Biometrics is about control, not security.

Try to get your Social Security number out of the “credit reporting” system. Impossible? It is impossible because of database sharing. REAL ID and systems used by DHS, would link the databases of states and nations. Linked databases would PERMANENTLY enroll Christians in a system, similar to one of Revelation 13. A system God will condemn. What greater threat to religious freedom is there than this?

SPECULATING ABOUT THE FUTURE

We may speculate over what kind of event would prompt the world to adopt the “mark?” ID theft? The potential of ID theft, in such an enormous global system, is mind-boggling. For such risks to be ignored by DHS and Congress defies explanation. But, a global ID theft pandemic COULD, prompt the introduction of “*other technological solutions*” where one is identified from birth using a mark. *Even under REAL ID, DHS will have the power to restrict buying, selling and moving, unless the individual has a biometric ID. Once databases are linked, we cannot get out, solidifying that control and power over our lives.* It is therefore, conceivable how, a world in a financial disaster, might embrace “other technologies.”

HOW WILL CHRISTIANS ESCAPE THIS SYSTEM, WHILE THE WORLD IS ENROLLED?

U.S. citizens can stop REAL ID, biometrics and database linking in the U.S. We can also influence other nations to accept our non-biometric passports (even after we compelled other nations to adopt biometrics). If this system is the enrollment process for the “mark” then it is likely that it cannot be stopped globally. ICAO, and UN, influence is significant. ICAO began work on the biometric e-passport in 1995, long before 9/11. However, as Christians, we believe God will provide a way of escape that we may be able to endure (1 Cor 10:13).

In the United States we have constitutional rights protecting our religious freedom. It is therefore probable that the United States will become a safe haven, protecting Christians from enrollment while the rest of the world is enrolled. The irony, of course, is that we imposed this system on the world.

HOW CAN THIS SYSTEM BE STOPPED?

By February 2008, states must decide to defy REAL ID or participate in it, and request an extension. REAL ID goes into effect May 11th, 2008. Time is short! Therefore it is extremely important that all political and religious differences be put aside and all groups opposed to REAL ID, and biometrics, pressure U.S. and state law makers with a common voice. Stopping REAL ID, biometrics and database linking benefits all U.S. citizens. A “fix” on this scale requires the greatest cooperation from the greatest amount of people. Although much has been said about religious freedom in this document, and especially Christian teachings, these issues touch every U.S. citizen. Republican, Democrat, Independent, liberal and conservative, all citizens love their freedom and do not want international organizations or tyrannical departments running the country and destroying constitutional liberties.

This is not just a, First Amendment, religious rights issue. The ACLU may be more concerned about privacy and preventing illegal searching of personal information. But, Fourth Amendment privacy rights are also essential to religious freedom. Stopping illegal searches, stops global database linking. Protecting religious freedom depends on states retaining control over DL/ID cards (Tenth Amendment)--- no national or international DL/ID. The Tenth Amendment limits federal powers and protects our access to the more “flexible” powers of state government, thus protecting our rights to representation on a local level. The right of representation is permanently damaged by this system since we have no representation with other nations or international organizations. Furthermore, once databases are linked, it is impossible to correct, making it impossible for a redress of grievances (First Amendment). So, our First Amendment religious rights are interconnected with other rights. All U.S. citizens share those rights. There is much room for common ground and agreement. However, we must be focused on the real solution that serves the common good.

We must stop biometrics, database linking-sharing and stop the influence of international organizations on U.S. law and government agencies.

Several things must happen to dismantle the biometric machine that has been growing since 1986. Below are some proposed solutions.

Nationally –

- 1 REPEAL REAL ID and other ID laws that depend on biometrics.

- 1 Wipe existing biometric information from passport, government employee ID records, military ID and related databases. Another possibility is to “permanently degrade” stored images so they are no longer usable with facial image recognition.

State level –

- 2 Wipe high-resolution facial images and any biometric fingerprints from existing DL/ID databases.
- 3 Replace existing biometric equipment with non-biometric systems that is limited to low-resolution facial images (no more than 25 pixels between eye centers --- current biometric ICAO standard is 90 pixels between eye centers). The purpose of this change is to make images “human readable” not “machine-readable.” This makes, existing and future facial images unusable for biometrics and pushes out the window for another “take-over” of state ID, at least 4-10 years, depending on the renewal cycle of each state. Using lower resolution images, even with sophisticated tamper resistant documents, will save this nation millions and millions of tax dollars that can be spent on REAL security.
- 4 Based on vendor claims and actual results, states and federal agencies should consider financial recovery against biometric vendors that misrepresented their products to obtain contracts.
- 5 Permit residents to OPT-OUT of photo and/or Social Security Number retention by state DMV-DPS (NH Model). This makes the state database incomplete of photo images, making it far less valuable for biometric enrollment or federal take-over in the future. This also protects privacy. If state DL/ID cards are securely designed, states do not need to retain the information, once the card is issued.
- 6 Permit residents to use mailing addresses, instead of physical addresses (required by REAL ID).
- 7 States must decide what technologies are best for ID document security, but without biometrics or data storage technologies like RFID chips and 2-D barcodes.
- 8 ID “breeder” documents, such as birth certificates can be made more secure and verified directly with the issuing agency. We do not need a DHS or AAMVA database or information clearing-house.
- 9 Businesses and schools, using biometrics must notify workers, visitors, students, parents of students, etc. of its use of biometrics, and create non-biometric ID document alternatives for employees, students, etc.
- 10 Hospitals must notify, parents of newborn babies, of any biometric uses (no more ink) and provide a non-biometric alternative.

Nationally and on a state level –

- 1 U.S. citizens must reclaim their government from the influence of international organizations such as AAMVA and ICAO. Typically, law makers create legislation, and the appropriate department promulgates the regulations. However, the dangerous influence of AAMVA and ICAO, has infected state and federal agencies and must be stopped. We have no hope of correcting this threat unless the influence of such organizations is addressed and control over government agencies is restored.

DO IT –TIME IS RUNNING OUT

The mission of Christians and pastors should be to speak-up and oppose this threat. Many hesitate to do so because of the complexity of the subject. Don't speak of complexity. Speak your conscience. Does it threaten your beliefs to be enrolled in this system? If yes, then the law must be changed, not the belief. PERIOD.

Simply tell law makers (U.S. and state) that REAL ID, biometrics, database linking and the influence of international organizations over state and U.S. law, threaten your religious rights. You will be shocked. Many U.S. and state law makers do not know of these issues. It is up to you to tell them. Encourage them to contact law makers in other states that have successfully stopped REAL ID. Simple letters and emails to law makers send a huge message. Bring their attention to this overlooked issue and also confirm the threat to religious rights. These letters and emails DO NOT require technical knowledge, but the sincere voice of concern. Pastors are especially powerful. Their voice, in the mind of the law maker, represents dozens or thousands of voters. Aggressively, stand for your constitutional rights, or you will lose them

Pastors, tell your congregation. Protect them from this threat. People are available to educate. Short

handouts and other materials can be distributed. Because many large Christian organizations have failed to address this issue, the international ID-biometrics-religious issues have largely been ignored in the mainstream. Individuals and pastors must petition these large organizations and their own denominational headquarters to immediately oppose this issue. Today, several groups, Senators, Congressman, state law makers, etc. have the information now and are investigating it with great concern. God is on our side.

REFERENCE PAGE

-
- ⁱ Source AAMVA – “Current and Ongoing Efforts – <http://www.aamva.org/KnowledgeCenter/Standards/currentandongoingefforts-biometrics.htm>
- ⁱⁱ Source ICAO – Tag/Mrt d17_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
- ^{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/Mrt d17_WP016.pdf (Jan. 2007) 3.1 Creation of ICAO
- ^{xii} Source ICAO – Tag/Mrt d17_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

^{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/SB112077340#647880052-cKyZgAb0T3asU4UDFVNPWrOAqCY_20060708.html

^{xix} Source ICAO – TagMrtid17_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://fvt.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

- 1 The “**Commercial Motor Vehicle Safety Act of 1986**” attempted to impose biometrics on state ID for identifying commercial driver’s license holders
- 2 **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)
- 3 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
- 4 “**Enhanced Security and Visa Reform Act of 2002**” – biometrics collected on visa holders - Visa Waiver nations issue biometric passports designed by ICAO

-
- 5 **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 AAMVA.net)
 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.

 - 1 **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

 - 2 **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 Moczny (DHS-US Visit) stated that global data sharing would begin with Europe, Asia (GCN February 5th, 2007).