

I want to thank the committee and the chairman, Senator Folmer for the opportunity to address the issues of the Real ID Act 2005 and biometrics.

My name is Mark Lerner. I am the Co-Founder of the Stop Real ID Coalition and a spokesperson for the Constitutional Alliance. Both groups are non partisan and consist of state lawmakers, national and state groups and private citizens. We have worked with both the ACLU and the ACLJ. I went to Virginia Beach on behalf of state lawmakers from Oklahoma to ask the ACLJ to take a position on the Real ID Act 2005. They did respond with a 117 page document opposing the Real ID Act and the use of biometrics. The ACLJ position paper has been submitted to the committee in the form of written testimony.

Biometric is defined as a measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee. Typically one thinks of fingerprinting, facial recognition or iris scanning when thinking of biometrics. For the purpose of today's hearing I will focus primarily on facial recognition. Facial recognition is measurements of different facial characteristics of the face. The digital facial image or picture is a biometric sample by definition, if the digital facial image can be converted to biometric data. The data that represents the biometric measurements of an enrollee is the template that is used at subsequent times against other templates to determine if there is a match.

Currently nations of the world are identifying their citizens using an international facial biometric identification system. This system is built on commonly used standards for identification and documentation to insure global interoperability that results in global information sharing. Biometric identification is linked to individual's personal information.

Consider the following which comes from a GCN (Government Computer News) article two years ago.

“Senior DHS officials speaking at a recent conference on biometrics and privacy policy outlined the ethical imperative for technical standards that would foster unrestricted biometric data sharing.

And while they say they recognize and agree with the need for privacy policy, threats of terrorism require governments and private companies to completely eliminate barriers to biometric data sharing.

Robert Mocny, acting program manager for the U.S. Visitor and Immigrant Status Indicator Technology program, sketched the outline of a Global Security Envelope of internationally shared biometric data that would permanently link individuals with their personal data held by governments and corporations.”

There are those that would argue if a person has nothing to hide then that person should not oppose whatever measures the federal government wants to take to protect us from acts of terrorism. I would suggest that if one was to read the Federalists Papers or the Constitution, the only conclusion that can be reached is our forefathers believed in the principle of the presumption of innocence. A person is innocent until proven guilty.

**“The essence of Government is power; and power, lodged as it must be in human hands, will ever be liable to abuse.” James Madison**

Democrats and Republicans have been guilty of accusing one another of being domestic terrorists or at the least of being unpatriotic and warranting investigation. I have included in my written testimony a recently made public document from DHS that speaks to the belief that certain right wing groups should be given special consideration for investigation of being comprised of potential domestic terrorists. There should be no wondering about why Americans are concerned that they are being treated as terrorists rather than just being citizens exercising their right to disagree with federal government’s policies and laws.

By being reliant on biometrics we are creating a recipe for disaster. Abuse of power has taken place at the federal level many times over the decades. In the last eight years we witnessed the abuse of National Security Letters by the FBI. A document corroborating that allegation is included in the written testimony. Most of us are familiar with the abuse of the Foreign Intelligence Surveillance Act. I have included an article in my written testimony describing what former NSA analyst Russell Tice has revealed about our telephone conversations, emails and even financial transactions being monitored by the NSA.

DHS has invested hundreds of millions of dollars in digital CCTV/surveillance technology. Cameras are going up all across the country. One might believe that the use of facial recognition technology and CCTV technology used simultaneously is Orwellian, it is not. Several times since 9/11 different biometric vendors and law enforcement agencies have used the two technologies simultaneously in real time. DHS started a program called Project Hostile Intent. The basic concept is computer software assesses whether or not a person is more or less likely to be a threat based on how the person behaves. The American Psychological Association submitted testimony to Congress that Project Hostile Intent was real time compatible. Imagine CCTV/surveillance cameras, facial recognition and Project Hostile Intent being used simultaneously in real time. Call it a surveillance society, police state or what you will. Some analyst behind a monitor will be utilizing all these technologies while at the same time “pulling up” information contained in multiple databases, including motor vehicle databases and databases that contain information about each of us collected by data mining companies.

The FBI wants to create the world’s largest biometric database. The Real ID Act, TWIC (Transportation Workers Identification Credential), E-Passport, EDL’s, passport cards and other identification documents all enroll Americans into the global biometric identification system I have been speaking of. Only Real ID or whatever wolf dressed in sheep’s clothing that replaces Real ID will insure that nearly all Americans are enrolled into this global biometric identification system.

The federal government wants all Americans enrolled into a single global biometric identification system that by its very nature will control a person’s ability to buy, sell and travel. There is a reason that facial recognition is the biometric of choice. It does not require that the subject knows the technology is being used. The term used to describe this lack of transparency is “non invasive”. Fingerprinting enrollment is invasive because it does require the subject’s participation, putting their fingertips on a scanner or placing ink on the fingertip to obtain a fingerprint.

Most Americans would agree there is a need for state driver’s licenses to have document integrity. Counterfeit driver’s licenses are not acceptable or are

licenses obtained as a result of an individual presenting fraudulent breeder documents. There are technologies such as watermarking that provide a high degree of document integrity.

The emphasis of our government should be on doing the best possible job of insuring breeder documents necessary to obtain a driver's license are authentic not in enrolling all Americans into a global biometric identification system.

A low resolution facial image can be human recognizable but not facial recognition compatible. If a police officer was to pull over a person without their driver's license or another form of identification, the officer could have a low resolution picture that is human recognizable provided from a DMV database and know if the person was telling the truth when providing his or her name.

We may identify some people that have multiple driver's licenses under different names with the use of facial recognition but if we insure breeder documents are authentic there is very little likelihood of a person obtaining multiple licenses under different names.

DHS released a Twenty Questions and Answers document in March 2007 at the same time that DHS released its NPRM (Notice of Proposed Rulemaking) for the Real ID Act 2005. Buried in the NPRM on page 68, footnote 17, is the standard a state must adhere to for the digital facial image or photograph of the driver's license applicant. That standard is the adopted standard of the International Civil Aviation Organization, an agency of the United Nations. That standard is to insure compatibility with facial recognition technology. With regard to the aforementioned Twenty Questions and Answers DHS stated they were not requiring states to collect any biometric data that they, the states, were not already collecting. As I stated earlier biometric samples are what is needed to create biometric data. Simply, DHS was splitting a hair that simply cannot and should not be split. I have included the Twenty Questions and Answers along with the Real ID Act 2005 NPRM in my written testimony.

Even if one would not agree there are those that are proponents of biometrics that are seeking "control" of the public then consider the following and ask if

control is not primary motivation for the use of biometrics, is commerce, or more precisely, protecting the bottom lines of multinational corporations?

DHS named AAMVA (American Association of Motor Vehicle Administrators) the “hub” and “backbone” in the final rules of the Real ID Act released by DHS in January 2008. AAMVA is an international organization that has promoting the use of biometrics long before 9/11. Neither the federal government nor any single state has jurisdiction over AAMVA. It is true that currently AAMVA is comprised primarily of Department of Motor Vehicle administrators from the states of the United States. That being said AAMVA has every intention of expanding. As AAMVA does expand U.S. influence will lesson and the interests if the United States will become less the priority. Currently all but a few states including the Commonwealth of Pennsylvania belong to what is known as AAMVA’s DLC (Driver’s License Compact). In simple terms the compact calls for states of the United States and provinces of Canada to make accessible information pertaining to citizens in each other’s jurisdiction. In 1994 when NAFTA was signed by President Clinton AAMVA first started considering what is known today as the DLA (Driver’s License Agreement). Among several differences between AAMVA’s DLC and its DLA is the jurisdiction change to include the districts of Mexico. Nearly all citizens I know are opposed to having their personal information either directly or indirectly accessible to Mexican districts of which many are controlled by drug cartels or been infiltrated by drug cartels. DHS’s position is that states are not required to participate in AAMVA’s DLA. I have submitted a comparison between AAMVA’s DLA and its DLC which clearly shows only AAMVA’s DLA can meet the majority of requirements of the Real ID Act 2005 and even the DLA requires some modification.

It is no coincidence that NAFTA and AAMVA’s DLA both occurred in the same year 1994. It is no accident that in 2005 when the Real ID Act was signed into law AAMVA’s DLA was revised. It is also not a coincidence that in the same year, 2005, the Western Hemisphere Travel Initiative was enacted. With the Western Hemisphere Travel Initiative came the EDL (Enhanced Driver’s License). The EDL is the sister to the Real ID compliant driver’s license. Two differences between EDL’s and a Real ID driver’s license are EDL’s can be used to cross borders and EDL’s utilize RFID technology. Secretary of Homeland Security Napolitano has been quoted as saying she would like all states to issue EDL’s.

Multinational corporations need seamless borders to reduce cost. If every person and all goods entering our country were thoroughly inspected it would slow down commerce. Slowing down commerce negatively impacts the bottom line of corporations. We do not need biometrics. What we do need is secure borders and more border checkpoints. If ICE (Immigration and Customs Enforcement) had more people we could have more border inspection checkpoints. That would help to reduce congestion at checkpoints if we did a thorough job of inspecting people and goods. It would also assist in preventing illegal drugs from entering our country. Security is not about convenience or being expedient. Security must be real not perceived.

We do not have the biometric samples or data of most terrorists. According to our own intelligence agencies hundreds of thousands of terrorists have been trained by groups such as Al-Qaeda and Hezbollah. What is important is for those charged with protecting our borders that they know when a person presents a document such as a passport, the document is authentic and has document integrity. If a document has document integrity then by definition the photo on that document cannot be altered or changed.

Some Governors have entered into agreements with DHS and the State Department to allow the Governors to issue EDL's in their respective states. There is no need for EDL's. The Government Printing Office pays \$7 or so for a passport and sells them to the State Department for roughly \$15. There is no reason for a 600% plus markup to citizens. The same is true for passports cards. Passport cards can legally be used to leave and enter the United States and can be offered at a very reasonable cost. EDL's are simply another way for the federal government to involve itself in the issuance of state driver's licenses. I would be happy to do discuss the numerous issues surrounding the use of RFID technology in identification documents at another time or upon the committee's request.

Last year I was present here in Harrisburg when Darrell Williams, DHS's Real ID program director testified that there was no relationship between the federal government and AAMVA. Mr. Williams went on to say what states and AAMVA do is between them. With all due respect to Mr. Williams he is wrong. I have

provided with my written testimony a document that clearly shows the federal government has been issuing grant money to states since 2006 for the purpose of encouraging states to participate in AAMVA's DLA. Many Americans I dare say would be outraged to know this is how their tax paying dollars are being used.

At some point we must consider developing a system for states and territories to share information about each other's drivers that does not involve AAMVA. We must protect our nation's sovereignty and not place our security in the hands of an international organization.

Those I represent would believe the federal government should not be involved in the issuance of state driver's license.

One problem is the Real ID Act and specifically the use of biometrics is there is no transparency. There should be full transparency which is why I recommend that FIPP(Fair Information Practice and Principles) be codified so that citizens know what information is being collected, how long the information will be retained, what the information is being used for, who the information can be shared with.

The organizations I represent support our law enforcement officers, our military and our intelligence community. If they need additional personnel or financial resources they should have them. What we oppose is the strategy of collecting any and all personal information of all citizens and making that information available to federal agencies and departments without proper cause. In addition we oppose the sharing of Americans personal information with foreign entities whether they are governments or international organizations unless some level of probable cause exists. There is a reason for court orders and specifically for the Fourth Amendment being included in our Bill of Rights.

Real ID was never voluntary. With the unfettered discretion provided the Secretary of DHS, restrictions covering nearly every aspect of our lives can be implemented. This unrestricted use of "restrictions" amounts to coercion. The Secretary of DHS can "restrict" gun ownership, prescription drugs and other areas if a person does not have a Real ID compliant driver's license. Yes, other alternative documents that require the same types of information including

biometric facial samples under the Real ID Act can be used to enter federal buildings, fly commercially or enter nuclear facilities.

I can appreciate the argument that there can be a need for the use of biometrics. If our government has a database of terrorists biometric samples or biometric data then check all people entering our country against such a terrorist biometric database. If a citizen is convicted of a crime then it would be appropriate to have the individual's biometric information.

Information is power. The federal government is using states as surrogates to collect information.

The National Governors Association and the National Conference of State Legislators are negotiating with DHS and members of Congress on legislation that would repeal Real ID Act. I assure you of one thing-Whatever replaces Real ID will include a mandate for the collection of facial biometric samples.

Some Governors and state lawmakers are afraid of losing grant money or stimulus money if they stand up to the federal government. Liberty is not for sale.

Going back throughout our country's history many including our forefathers, Paul Harvey, President Kennedy and others have warned that the greatest threat to our freedom comes not from external forces but from our own government. President Reagan and other Presidents have stood tall against a national ID card.

We are moving towards having the driver's license becoming a one shoe fits all sizes document. We use it to cash checks, before we can buy or sell goods or services, and with EDL's to cross borders. Pilot programs have taken place that removes the need for cash or credit cards. The driver's license is "swiped" and money is electronically removed from a person's bank account. L-1 Identity Solutions, the vendor for the Commonwealth of Pennsylvania had a web-page titled "Real ID Solutions". On the web-page they had a sample of what one can only presume the company believes a Real ID driver's license would look like. On the front of that sample driver's license is the person's political party affiliation. I have submitted that example with my written testimony. I am appalled at the idea that L-1 thinks every time we are asked for our driver's licenses we should be

compelled to reveal our political affiliation. A person's political affiliation is that person's business unless the person chooses to make it known. The more we rely on driver's licenses to exist in everyday life, the more we put at risk our personal information that is contained in state DMV databases.

The groups I represent do not focus on individual elected leaders or their appointees. We do not focus on political parties. We believe there is a "culture" that does exist that engulfs those in decision making positions that does ignore basic principles of our society and/or our Constitution. State lawmakers are by design a citizen's line of defense against federal tyranny.

I would ask everyone to remember our allies of today can become our enemies of tomorrow. Think of Saddam Hussein and you have to look no further. Global information sharing must only take place when there is a specific reason related to specific people.

Yes, we could be safer if we placed a police officer or even soldiers on every block. We could decide that no communications would be protected from eavesdropping. If there was a crime every possible person could be given a polygraph. We could do many things but the point is-With freedom comes risk.

Stop the collection and use of biometric samples and data in Pennsylvania. Remove existing biometric information unless the information was acquired as a result of a search warrant or unless a person has been convicted of a crime. The next time we witness an abuse of power we may not be able to undo the harm. Think of instances of abuse of power in the past and then imagine if those that abused power had the laws and technologies that exist today.

Do not confuse freedom with lifestyle. By the time you realize your lifestyle has been altered because your freedom has been taken from you it will be too late.

We are turning rights into privileges. Yes, arguably driving is a privilege but it is also a necessity. Government should not take advantage of citizen's rights when there is a real necessity for citizens to participate in an activity. Driving is such an activity and government is taking advantage of the fact driving for most Americans is a necessity.

Lawmakers must stop considering each law and the use of technology that comes with that law as separate legislation but rather must start considering the totality of all the laws and the uses of technologies that come with those laws before creating more laws. We must consider expected advancements in technologies that we allow to be used today. It is a fact that we as a country have become very good at stating what privacy does not mean but I am afraid we are not equally proficient at defining what privacy and liberty do mean. The type of society future generations of Americans live in will be determined to a large extent by the actions we as a country take today.

Thank you,

Mark Lerner

