

REAL ID — “A Global Security Envelope”

By Amanda Teegarden • OK-SAFE, Inc. • March 2008

“The purpose of law is the defense of life, liberty, and property.” —*The Law*, by Frederic Bastiat, p. x

The REAL ID Act of 2005 is a federal government attempt to *standardize* all state issued drivers’ licenses and personal identification cards, in order to allow US citizens to board a federally — regulated airplane or access a federal facility, presumably to stop terrorism and prevent fraud.¹

These would be the same federal facilities for which the US taxpayers have already paid, but for whom the government wants to restrict access.

What the REAL ID really does is invade the privacy of (and creates biometric profiles for) law-abiding US citizens; adds to an ever-increasing surveillance system monster called *security*; and lines the pocket books of *insider* former government officials.

All this while the Department of Homeland Security is in charge.

Privacy...

“Under REAL ID, all new licenses would be machine-readable and contain personal information that could be scanned by governments and potentially by corporations.”²

The biometric data and the other personal data become part of both a national and international database of information, accessible not only by state agencies, but by the federal government and foreign governments, including Mexico and Canada.

Did anyone ask the American people if they wanted to be part of an internationally shared biometric database? What arrogance on the part of the federal government and their agencies to trample on the rights and dignity of the American people.

“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.”

“Mocny sketched a federal plan to extend biometric data sharing to **Asian and European** governments and corporations, so as to create a **Global Security Envelope** of identity management.”³

Bio means life...

Biometrics means using technology to measure biological information. This includes “1) scanning the anatomy being used, 2) the software to gather the information and convert it to digital form, and 3) the database to compare to stored data and determine authenticity and identification.”⁴

There is both physiological biometric data and behavioral biometric data.

Physiological biometric data includes:

- Facial feature pattern characteristics*
- Fingerprints*, palm prints, and other methods for measuring or recording ridge pattern or fingertip characteristics
- Retinal scans
- Hand geometry, measuring hand characteristics, including shape and length of fingers
- Deoxyribonucleic acid (DNA) and/or ribonucleic acid (RNA)

Behavioral biometrics includes:

- Voice data used for comparing live speech with a previously created speech mode of a person’s voice
- Behavior characteristics of handwritten signature, such as shape, speed, pressure, pen angle, or sequence
- Keystroke dynamics, measuring pressure applied to keypads.⁵

* Photos using facial-recognition and fingerprints are part of the requirements of the Oklahoma Department of Public Safety to obtain a state issued Drivers’ License or Identification card.

Surveillance systems...

This biometric database, fed by sources such as drivers’ license photos and fingerprinting, fits right in with the technology systems in place in other sectors — such as the global tracking systems for transportation and freight management. The same technology that scans a freight carrier can scan a vehicle and the passengers in it — and without their knowing.

Lockheed Martin has developed an “Information Integration” system called **Total Domain Awareness**, that:

“Automatically gather, correlate, and interpret fragments of multi-source (Radar, AIS & GPS tracks, Open Source, Intelligence, Watch List & Law Enforcement Report, CCTV, Bioterrorism sensors) data together into one collaborative portal-based environment.”⁶

What this means is every move made by any vehicle, whether truck, sea vessel, rail, or passenger car, can be tracked everywhere at anytime, in real time.

NASCO, North America's SuperCorridor Coalition, is promoting **Total Domain Awareness** their special project called NAFTRACS by SaviNetworks of Lockheed Martin.

This is made possible by the collection of data from multiple sources; the linking of data and the software making the systems compatible and the information accessible — for a fee — to governments, foreign and domestic, their agents, and/or the private sector.

It's all about money...

In February of 2003 Oklahoma announced it had signed a \$12 million contract with Viisage Technology, Inc. for the digital drivers' license contract.

"The solution, developed by Viisage, will integrate multiple, advanced identification security features, including its FaceEXPLORER™ facial recognition software and SAGEM Morpho finger imaging technology."⁷

The Oklahoma announcement came just before the May 2003 press release when Viisage Technology revealed their participation in a security project for the United Arab Emirates, utilizing Viisage's facial recognition system "to enhance the integrity of the country's visa process."⁸

The UAE project involved using the same FaceEXPLORER™ software used in Oklahoma. Viisage Technology acquired Iridian and ZN Vision along the way, expanding their technological reach and depth.

In early 2003, supposedly there were quite a few facial-recognition technologies, but two were judged to be "competent" by the Department of Defense; Viisage Technology was one of them.

Viisage Technology, Inc., merged with Identix Incorporated in 2006 and became L-1 Identity Solutions, "with a potential market share of 80%, projected to reach \$3.5 billion by 2008."⁹

At about this same time, George Tenet (former CIA director), Louis Freeh (former FBI director), and James Loy (Deputy Secretary of Dept. of Homeland Security), were added to the 13-member board of Viisage.¹⁰

Is it any wonder that the Department of Defense acknowledged Viisage as competent?



Oklahoma objects...

In 2007, Oklahoma lawmakers passed SB 464, which states that **"The state of Oklahoma shall not participate in the implementation of the REAL ID Act of 2005."**¹¹

SB 464 further stated that the REAL ID "is inimical to the security and well-being of the people of Oklahoma, will cause approximately Eight Million Dollar (\$8,000,000) in added expense and inconvenience to our state, and was adopted by the United States Congress in violation of the principles of federalism contained in the Tenth Amendment to United States Constitution."¹¹

Governor Brad Henry supported SB 464 and signed off on this piece of legislation, which became effective on 11/1/07.

The bill further calls for the retrieval of "any biometric data previously collected, obtained, or retained in connection with motor vehicle registration or operation shall be retrieved and deleted from any and all databases" that had anything to do with the REAL ID.

Conclusion...

It is important for the citizens of Oklahoma to contact their legislators AND Governor Brad Henry and tell them you want no part of the REAL ID "Global Security Envelope."

Biometric information belongs to the individual, not the state, and should not be shared with other agencies, other countries, or any corporations.

To find you Legislator click here. Or call 1-800-522-8502. To contact Governor Brad Henry, click here. Or call (405) 521-2342.

Endnotes:

- 1 Known as Public Law 109-13, The Emergency Supplemental Appropriations for Defense, the Global War on Terror, Tsunami Relief Act of 2005 included provisions for the REAL ID Act of 2005.
- 2 "ID Plan is Broadly Criticized, Bipartisan Objections Cite Security, Costs, and Privacy," by Dafina Linzer, *Washington Post* Staff Writer, Saturday, Jan. 12, 2008.
- 3 "DHS pushes global data sharing," by Wilson P. Dizard III, Jan. 5, 2007 http://www.gcn.com/print/26_03/43061-1.html
- 4 <http://webhost.bridgew.edu/jcolby/it525/definition.html>
- 5 *ibid.*
- 6 OK Open Records, NASCO Corridors of the Future Proposal, 2006; Available at www.ok-safe.com
- 7 "Viisage Receives \$12 million Award from the State of Oklahoma," Feb. 2003; http://www.findbiometrics.com/Pages/news_releases/news311.html
- 8 "Viisage Technology to Provide Facial Recognition Solutions to United Arab Emirates," May 2003, http://www.findbiometrics.com/Pages/news_releases/news450.html
- 9 "The merger positions the new company as a market leader in the biometrics sector. The combined capabilities allow the new company to effectively compete for approximately 80 percent of a market opportunity projected by Frost & Sullivan to reach \$3.5 billion by 2008*." <http://apps.shareholder.com/secviewerContent.aspx?companyId=LONE&docid=5033465T>
- 10 *Stiegele v Bailey et al of Viisage Technology* <http://pacer.mad.uscourts.gov/dc/cgi-bin/recenttops.pl?filename=wolf/pdf/stiegle+opinion3.pdf>

**Visit our website:
www.ok-safe.com**