

SAMUEL E. ROHRER, MEMBER
128TH LEGISLATIVE DISTRICT
ROOM 45 EAST WING
PO BOX 202128
HARRISBURG, PA 17120-2128
PHONE: (717) 787-8550
FAX: (717) 783-7862
srohrer@pahousegop.com

DISTRICT OFFICE:
29 VILLAGE CENTER DRIVE, SUITE A7
READING, PA 19607
PHONE: (610) 775-5130
FAX: (610) 775-3736
www.samrohrer.com



House of Representatives
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

GAME & FISHERIES,
REPUBLICAN CHAIRMAN
EDUCATION
SPEAKER'S COMMISSION
ON LEGISLATIVE REFORM

CAUCUSES

EAST CENTRAL CAUCUS
PA LEGISLATIVE SPORTSMEN

January 23, 2008

The Honorable Edward G. Rendell
Governor
Commonwealth of Pennsylvania
225 Main Capitol Building
Harrisburg, Pennsylvania

Dear Governor Rendell,

In the wake of the REAL ID Act of 2005, a renewed interest in security and privacy issues has forged a unique coalition which crosses party lines and political divides. Legitimate concerns over continued encroachments on privacy rights mandate that we, as stewards of the Commonwealth's constitution, consider anew any policies which impact on these cherished values.

This letter, while related in some ways to the parameters of REAL ID implementation, is generally focused on the current agreements between Viisage Technology and the Pennsylvania Department of Transportation (PennDOT) encompassed in Contract 359820, its supplements and associated materials. Some questions are specific to the main contract or one of the many supplements, while others involve concerns which exist in all of the twists and turns of Contract 359820.

Background

Viisage Technology (Viisage) describes itself, in materials submitted to PennDOT in 1999, as "the industry leader in instant issue digital driver's licenses, producing nearly 50% of all U.S. over-the-counter (*sic*) driver licenses." Beginning in 2000 with Contract 359820, Viisage and PennDOT entered into a series of agreements to provide for digitized driver licensing, technological updates and other goods and services. This letter asks significant questions about the statutory authority for various contractual terms as well as the adequacy of security measures associated with these contracts.

According to information on its website, the American Association of Motor Vehicle Administrators (AAMVA) is a nonprofit organization which "represents state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws." The

membership also includes “associations, organizations and businesses that share an interest in the association’s goals.” While your administration and PennDOT are obviously aware of the makeup and purpose of the AAMVA, it is important to include the aforementioned descriptive material in order to set the appropriate context for the discussion which follows. In particular, it is the existence of the AAMVA as a private, rather than a government, entity which gives rise to the concerns expressed throughout this letter. The issues raised in this letter are not intended to impugn the motives of the AAMVA or its membership. They are, however, intended to question the statutory authority of a nongovernmental, international organization to access protected personal information and establish standards for Pennsylvania driver’s licenses.

General Questions

There are a number of general questions which will be useful to frame some of the basic issues as we move forward.

- What is the current standard for image quality in driver’s license images?
- How was that standard developed? Is it an AAMVA standard?
- What is the accepted human-readable standard in driver’s license imaging? If this differs from the current standard used by PennDOT, what is the cost difference (computer storage, etc.) between the use of the current standard and the use of a human-readable standard?
- Who has access to driver’s license information maintained by PennDOT, e.g., JNET, other states’ departments of motor vehicles, etc.? What is the statutory authority to allow sharing of this information?
- What information is maintained on the machine readable technology (bar code and magnetic stripe) on the back of a driver’s license? Is this information encrypted? Are Social Security numbers part of the information maintained on the machine readable technology? Are any biometric images (fingerprints, photos and facial measurements, etc.) on the machine readable technology? Are there plans to include biometric images, Passport information or medical information?

Security

According to documentation supplied by PennDOT, there are legitimate factual questions about the security performance of Viisage. For example, in October of 2001 it appears that Viisage failed to comply with contractual security provisions regarding staff background checks. In 2002, Viisage delivered a shipment of holographic overlays, one of the primary security measures used in the creation of Pennsylvania driver’s licenses, to a private business rather than a photo license center.

- Have there been other breaches of security protocols by Viisage during the course of any contract with PennDOT? If so, what are the details?

- How have all of these issues, including the two aforementioned examples, been addressed by Viisage and PennDOT? Please provide any documentation available to supplement answers.
- Is there a comprehensive security plan? Does it describe proper handling, storage, disaster, recovery, and dissemination processes? Does security include physical as well as human engineering concerns? Does it provide for the secure destruction of any and all originals or backups under the control of any private entity upon the termination of contract 359820 such that no privately held copies remain in public domain? Please provide a copy of any such plan.

Sensitive, personal information concerning licensed Pennsylvania drivers should be maintained under strict and comprehensive security measures. The various documents associated with Contract 359820, which outline the ongoing relationship between Viisage and PennDOT, discuss the use of Viisage storage facilities to hold private data found in Pennsylvania driver's license records. In the Viisage Proposal of November 1999, there are numerous references to the Central Image System and backup data being held at Viisage, rather than PennDOT, locations. In Contract 359820 – Supplement C, there is discussion of moving the backup central image system out of the Commonwealth of Pennsylvania. This is particularly troublesome.

- What records of driver's license information, including backup records, are maintained at Viisage facilities or other non-governmental sites?
- What is the statutory authority to allow this information to be maintained by a private entity?
- What is the benefit to maintaining driver's license information at private facilities?
- Where are those facilities located?
- What security measures are in place at these private facilities and how are those measures verified?
- How often do PennDOT personnel inspect the private facilities which contain driver's license information? And what is the scope of such an inspection?
- Is Viisage allowed to share or provide, with or without a fee, such information to any third party, domestic or international? Do any statutory limitations, contractual terms or other protections exist to prevent such sharing of information?
- Should Pennsylvania law fail to accept the terms of the Real Id Act of 2005, would Viisage be legally or contractually bound to adhere to Pennsylvania state law or Federal law with regard to relinquishing Pennsylvania records to any Federal authorities or other states?

Biometric Identifiers – Facial Images – Facial Recognition

Another concern raised by REAL ID implementation involves the privacy interests in facial images. Specifically, Contract 359820 – Supplement C memorializes an ongoing effort to establish the use of biometric identifiers as part of the Viisage FaceEXPLORER program. The language of Supplement C notes one of the goals of this effort is to “provide capability to create biometric FR templates.”

- What is the statutory authority to engage in the FaceEXPLORER program or similar facial recognition programs? How have constitutional issues related to privacy been addressed?
- How complete is the implementation of FaceEXPLORER or any similar facial recognition program by PennDOT? What percentage of current licensing images have been created as, or converted to, facial recognition templates?
- Has there been any testing to determine the success rate of FaceEXPLORER?
- What are all the uses, currently and those planned for implementation, for FaceEXPLORER and its investigative browser?
- Where are records and backups maintained? Are any images or FR templates maintained at Viisage facilities? Where are those facilities?
- What controls are in place, including statutory limits on the use of driver's licensing information, to prevent FaceEXPLORER (or similar programs) and the associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?

DIEP Pilot

Contract 359820 – Supplement D authorized additional services for digital image exchange involving Viisage, the AAMVA and the Commonwealth. In particular, this supplement established involvement of all three parties in the Digital Image Exchange Program (DIEP) pilot project. We would ask for answers and supporting documentation for the following questions:

- What is the statutory authority to enter in to this agreement?
- What are the security parameters involved in the DIEP pilot?
- Since it is a pilot project, how have any security concerns been addressed regarding new requirements?
- Does the AAMVA have access to any driver's license information? If so, what is the statutory authority for allowing the AAMVA (a private entity) to view this information?
- What is the statutory authority to allow "digital image exchange standards" to be developed by the AAMVA rather than PennDOT? What standards have been established to date and why?

Conclusion

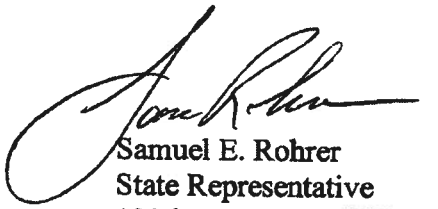
It is understood that PennDOT has a legitimate need to ensure appropriate identification of drivers and prevent identity theft. At the same time, these needs cannot trump a constitutional imperative that certain information is private and should only be surrendered for very limited, narrow governmental purposes. Further, it is vitally important that protected driver information is stored securely and is not transferred to private interests.

We sincerely appreciate PennDOT's veracity and the information provided to date concerning the Viisage contract and the many variations on this theme. Given the concerns and questions which have been raised, it would seem prudent to postpone the march towards implementation of facial recognition technology and the transfer of protected information to private entities until your administration is able to:


- answer the questions raised in this letter,
- provide references to the statutory authority for the actions discussed above, and
- ensure the security of otherwise confidential information which the citizens of Pennsylvania have provided to PennDOT for the very limited purpose of driver licensing.

Please forward the answers and supporting statutory references to Representative Samuel Rohrer's office, 45 East Wing, by Friday, February 8, 2008.

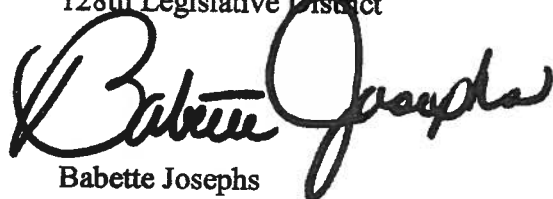
Sincerely,



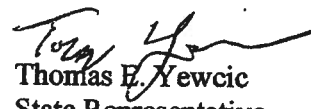
Samuel E. Rohrer
State Representative
128th Legislative District




John J. Siptroth
State Representative
189th Legislative District



Babette Josephs
State Representative
182nd Legislative District



Thomas E. Yewcic
State Representative
72nd Legislative District



Gordon R. Denlinger
State Representative
99th Legislative District

SER/bjj

cc: Allen D. Biehler, P.E.
Secretary of Transportation



COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF TRANSPORTATION
HARRISBURG, PENNSYLVANIA 17101-1900

OFFICE OF
SECRETARY OF TRANSPORTATION

February 15, 2008

Honorable Samuel E. Rohrer, Member
House of Representatives
Room 45 East Wing
PO Box 202128
Harrisburg, PA 17120

Dear Mr. Rohrer:

Governor Rendell asked that I respond to your correspondence dated January 23, 2008, requesting information on the current agreements between Viisage Technology and the Pennsylvania Department of Transportation. In order to ensure we have responded to all of your questions, I have listed your general concerns and each question below with our response.

General Questions

There are a number of general questions which will be useful to frame some of the basic issues as we move forward.

- Q. What is the current standard for image quality in driver's license images?*
A. Joint Photographic Experts Group (JPEG) for images and Tagged Image Format File (TIFF) for signatures.
- Q. How was the standard developed?*
A. These are non-proprietary industry standards that are used globally.
- Q. Is it an AAMVA standard?*
A. No. However, AAMVA recommends jurisdictions use these industry standards.
- Q. What is the accepted human-readable standard in driver's license imaging?*
A. AAMVA has published driver license/identification specifications. These specifications were developed by a committee comprised of representatives from various jurisdictions and industry segments for the purpose of assisting states when designing their DL/ID products. These are merely guidelines that jurisdictions can choose to follow if they wish. The human-readable elements that AAMVA recommends are name, date of birth, gender, driver's license number, address, image, signature, issue date, expiry date, eye color, height, class, endorsements, restrictions, duplicate counter, card type, and jurisdiction name.

- Q. If this differs from the current standard used by PennDOT, what is the cost difference (computer storage, etc.) between the use of the current standard and the use of a human-readable standard?*
- A. Pennsylvania driver's licenses/identification cards contain all the human-readable data elements recommended by the AAMVA specifications. In addition, it also contains the organ donor designation, when applicable, as required by Act 1994-102.
- Q. Who has access to driver's license information maintained by PennDOT, e.g., JNET, other states' departments of motor vehicles, etc.?*
- A. Pennsylvania law (Section 6114 of Title 75) permits the release of driver information in the following circumstances:
- Requestor has a signed release of the driver
 - Court order
 - To any Federal, State or local governmental agency for the sole purpose of exercising a legitimate governmental function or duty.
 - Of a constituent released to a member of Congress or of the General Assembly or to an employee of a member of Congress or of the General Assembly.
 - To a person who, in compliance with the Fair Credit Reporting Act, has filed with the department an affidavit certifying the intended use of said record.
 - To a messenger service which has filed an affidavit of intended use with the department and which maintains on file at its office of record an authorization in writing by the person who is the subject of the obtained record or report.
- Q. What is the statutory authority to allow sharing of this information?*
- A. Section 6114 of the Vehicle Code defines who is entitled to obtain driver information. This Section severely limits those who may have access to the information and the terms and conditions of such access. These are stricter limitations than required by the Federal Driver Privacy Protection Act.
- Q. What information is maintained on the machine-readable technology (bar code and magnetic stripe) on the back of the driver's license?*
- A. Prior to the recent technology upgrade of our photo license equipment, the driver's license contained a magnetic stripe, a two-dimensional barcode and a one-dimensional barcode. The magnetic stripe and two-dimensional barcode contain the same information that is printed on the front of the driver's license (name, address, DL#, issue date, expiry date, etc.) The one-dimensional barcode

contains the driver's license number only. Products issued after the technology upgrade include the above machine-readable technologies as well as an additional one-dimensional barcode that contains the serial number of the card. The technology upgrade began in October 2007 and will be completed in February 2008.

Q. Is this information encrypted?

A. No. The data contained in the machine-readable technologies (magnetic stripe, two-dimensional barcode, and both one-dimensional barcodes) is not encrypted.

Q. Are social security numbers part of the information maintained on the machine readable technology?

A. No. The social security number is not part of the machine-readable technologies contained on the driver's license/identification card.

Q. Are any biometric images (fingerprints, photos, and facial measurements, etc.) on the machine readable technology?

A. No. There are no biometric images included in the machine-readable technologies.

Q. Are there plans to include biometrics images, Passport information or medical information?

A. No. We have no plans to include any biometric images, Passport information or medical information in our machine-readable technologies.

Security

According to documentation supplied by PennDOT, there are legitimate factual questions about the security performance of Viisage. For example, in October 2001 it appears that Viisage failed to comply with contractual security provisions regarding staff background checks. In 2002, Viisage delivered a shipment of holographic overlays, one of the primary security measures used in the creation of Pennsylvania driver's licenses, to a private business rather than a photo license center.

Q. Have there been other breaches of security protocols by Viisage during the course of any contract with PennDOT? If so, what are the details?

A. In November 2006, the Wilkes-Barre Driver's License Center was burglarized and two computers used to issue driver's licenses were stolen. The thieves also took equipment and supplies that could be used to make fraudulent driver's

licenses/identification cards. During the investigation, PennDOT discovered the computers contained personal information of 11,384 customers who had their photos taken for a driver's license/identification card between August 30, 2006 and November 28, 2006. The information stored on the computers included names, addresses, dates of birth, driver's license numbers and the last four digits of Social Security numbers. In the case of 5,348 of those customers, the personal information included the complete Social Security numbers. The investigation also revealed that back-up tapes were being stored in an unsecured location. This matter is currently under investigation by the police and the Department is not at liberty to divulge additional information relating to the details of this event.

Q. How have all of these issues, including the two aforementioned examples, been addressed by Viisage and PennDOT? Please provide any documentation to supplement answers.

A. Below is our response for each of the items identified.

Background checks – When PennDOT learned that Viisage had employed individuals prior to the completion of the required background checks, Viisage was instructed to have all background checks completed. Viisage has supplied PennDOT copies of the completed background checks for their employees assigned to the Pennsylvania program. This is not information that can be released.

Delivery of materials - The incident of holographic overlay being delivered to a private business rather than a photo license center was a failure of UPS. The shipping label used by Viisage clearly states that no indirect delivery can be made. If a delivery issue is identified, it is immediately brought to the attention of UPS management and appropriate disciplinary action is taken against their employee.

Wilkes-Barre Burglary - PennDOT immediately required Viisage to reduce the time period data remained on the computers as well as encrypt the data. In addition, Viisage was instructed to eliminate the need to store any data for a completed transaction with the planned technology upgrade. The technology upgrade began October 22, 2007 and will be completed statewide by the end of February 2008.

PennDOT placed a stop on all records that were affected to eliminate any fraudulent activity from occurring. New driver's license numbers were issued to the customers whose personal information was contained on the computers. In

addition, PennDOT offered free credit monitoring for one year to all individuals impacted.

PennDOT also required Viisage to immediately secure the back-up tapes. They are now kept in a secure facility in Pennsylvania.

Q. Is there a comprehensive security plan?

A. Yes, a security plan is in place.

Q. Does it describe proper handling, storage, disaster, recovery, and dissemination processes?

A. The security plan includes information on how the data is stored, where the data is stored, how the data is protected and disaster recovery procedures. Contract 359820 governs the dissemination of information.

Q. Does security include physical as well as human engineering concerns?

A. The security plan describes the physical security features. If your reference to "human engineering concerns" means, are there checks and balances in place, the answer is yes.

Q. Does it provide for the secure destruction of any and all originals or backups under the control of any private entity upon the termination of contract 359820 such that no privately held copies remain in public domain?

A. Contract 359820, Requirement F – Central Image System of the RFP, specifies that all files and data are the sole property of the Commonwealth and upon contract termination Viisage must transfer all image files and any custom software required to read the image files to PennDOT.

Q. Please provide a copy of any such plan.

A. Although a security plan is in place that addresses security of the facility as well as the data, we respectfully decline to provide a copy. This information is confidential and its release would compromise the security measures in place.

Sensitive, personal information concerning license Pennsylvania drivers should be maintained under strict and comprehensive security measures. The various documents associated with Contract 359820, which outline the ongoing relationship between Viisage and PennDOT, discuss the use of Viisage storage facilities to hold private data found in Pennsylvania driver's license records. In the Viisage Proposal of November 1999, there are numerous references to the Central Image System and backup data being held at Viisage, rather than

PennDOT, locations. In Contract 359820 – Supplement C, there is discussion of moving the backup central image system out of the Commonwealth of Pennsylvania. This is particularly troublesome.

Q. What records of driver's license information, including backup records, are maintained at Viisage facilities or other non-governmental sites?

A. In addition to images and signatures, Viisage's Central Image Server contains all data that is printed on the front of the driver's license/identification card. Viisage also maintains data on behalf of the Department of State for the Motor Voter Program. For individuals that choose to apply to register to vote through the Photo License Program they maintain county, race, political affiliation and telephone number.

AAMVA manages the Commercial Driver License Information System (CDLIS). CDLIS is a pointer system that contains DL#, name, date of birth, SSN, "AKA" information, and state of record regarding commercial drivers.

Insurance companies get driver record information for their clients or persons seeking to obtain coverage, often through a consumer credit reporting intermediary such as ChoicePoint, under the authority of the federal Fair Credit Reporting Act. The consumer credit agencies are not allowed to warehouse that data but there is no such similar restriction on the insurance company as the legally authorized end user.

Q. What is the statutory authority to allow this information to be maintained by a private entity?

A. AAMVA manages CDLIS. CDLIS was created by the federal "Commercial Motor Vehicle Safety Act of 1986". The Act (49 U.S.C. 321309) required the federal Secretary of Transportation to establish or designate an entity to serve as a clearinghouse for all state jurisdictions. The Secretary designated AAMVAnet as the system operator. Thus, CDLIS is the designated arm of the U.S. Department of Transportation. Providing this information to CDLIS is authorized under Section 6114(b) (4) of the Pennsylvania Vehicle Code and Chapter 95 of the Department's regulations. In addition, federal law now mandates reporting of suspensions, etc, of all drivers to the conjunct National Drivers Register. 49 U.S.C.S. 30304 (2004). These actions are also reported to the Problem Driver Pointer System (PDPS), consistent with U.S. DOT regulations at 23 CFR 1327.1.

Participation in all of these entities is absolutely essential to enable the Department to fulfill the mandates of Pennsylvania law to limit persons to one license (75 Pa. C.S 1501(c)) and not to license those who are under suspension in another jurisdiction. (75 PA. C. S. 1503(a)(1).)

Q. What is the benefit to maintaining driver's license information at private facilities?

A. The Commonwealth has limited technical expertise and resources needed to develop or maintain the equipment and software required to issue photo driver's license/identification cards. Outsourcing this function is a cost effective solution that has allowed us to improve the security of the issuance process.

Q. Where are those facilities located?

A. The private facility provided under Contract 359820 is located in Pennsylvania. The back-up data is housed in a Commonwealth facility.

Q. What security measures are in place at these private facilities and how are those measures verified?

A. These facilities are secured. We respectfully decline to disclose the security measures in place because to do so would potentially compromise the effectiveness of our program.

Q. How often do PennDOT personnel inspect the private facilities which contain driver's license information?

A. PennDOT audits the Viisage facility twice a year.

Q. What is the scope of such an inspection?

A. PennDOT performs an inventory audit, reviews paperwork, and checks the building security.

Q. Is Viisage allowed to share or provide, with or without a fee, such information to any third party, domestic or international?

A. No. Viisage is prohibited from releasing any information without PennDOT's written approval.

Q. Do any statutory limitations, contractual terms or other protections exist to prevent such sharing of information?

A. Viisage is subject to the restrictions of Section 6114 of the Vehicle Code on the dissemination of driver license information. The Department has enhanced the restrictions in Section 6114 by expressly providing in Viisage's contract that it is

prohibited from selling, publishing or distributing the images or data without the written approval of the Commonwealth.

Q. Should Pennsylvania law fail to accept the terms of Real ID Act of 2005, would Viisage be legally or contractually bound to adhere to Pennsylvania state law or Federal law with regard to relinquishing Pennsylvania records to any Federal authorities or other states?

A. Whether or not Pennsylvania accepts the terms of Real ID Act of 2005, all data maintained by Viisage is the sole property of the Commonwealth and its contract prohibits it from releasing any image or data without the written consent of the Commonwealth.

Biometric Identifiers – Facial Images – Facial Recognition

Another concern raised by REAL ID implementation involves the privacy interest in facial images. Specifically, Contract 359820 – Supplement C memorializes an ongoing effort to establish the use of biometric identifiers as part of the Viisage FaceEXPLORER program. The language of Supplement C notes one of the goals of this effort is to “provide capability to create biometric FR templates.”

Q. What is the statutory authority to engage in the FaceEXPLORER program or similar facial recognition programs?

A. There is no impediment in the law that would prohibit the Department from using this very valuable tool.

Q. How have constitutional issues related to privacy been addressed?

A. The broad definition of biometrics includes facial recognition. This is a physically non-intrusive technology unlike DNA testing or fingerprinting. PennDOT utilizes facial recognition software as a tool to compare a customer’s photograph against our database of photographs to ensure the customer does not have another driver’s license issued under a different identity.

PennDOT has determined that the use of this tool is not a constitutional violation. Obtaining a driver’s license is a privilege. The state is entitled to condition the grant of that privilege on the individual’s consent to have their picture taken and used as necessary to protect security and for other legitimate government functions. It is PennDOT’s responsibility to take steps to ensure the integrity of the process, and facial recognition software is one tool we use to do that.

Q. How complete is the implementation of FaceEXPLORER or any similar facial recognition program by PennDOT?

A. All images have been compared utilizing the FaceEXPLORER software. The results are still being reviewed and analyzed by PennDOT staff.

Q. What percentage of current licensing images have been created as, or converted to, facial recognition templates?

A. 100 percent of all images.

Q. Has there been any testing to determine the success rate of FaceEXPLORER?

A. The FaceEXPLORER software utilized by Pennsylvania was tested by the National Institute of Standards and Testing (NIST) in 2006. Results of the test can be found at www.frvt.org.

Q. What are the uses, currently and those planned for implementation, for FaceEXPLORER and its investigative browser?

A. PennDOT currently uses FaceEXPLORER as a tool to help determine if an individual has more than one driver record. The images of all new applicants are compared to all existing images to identify possible matches. In addition, PennDOT is in the process of reviewing all images captured prior to FaceEXPLORER to determine if multiple records exist for one individual. After a comprehensive review has been completed and it is determined that the individual has more than one record, those driving records are cancelled.

Investigative browser is a fraud prevention tool utilized by the Department's Office of Risk Management and limited law enforcement agencies when conducting an investigation. It provides the ability to take a single image and compare it to all images on the database. This tool allows us to identify someone from their image as well as determine if the individual has established more than one identity.

There are no additional uses planned at this time.

Q. Where are records and backups maintained? Are any images or FR templates maintained at Viisage facilities? Where are those facilities?

A. All FaceEXPLORER data is maintained at the same locations that house the other data that is part of Contract 359820. As stated earlier, the Viisage facility is located in Pennsylvania. The back-up of this data is located at a Commonwealth facility.

- Q. What controls are in place, including statutory limits on the use of driver's licensing information, to prevent FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?*
- A. Please refer to the question and answer given earlier in reference to how PennDOT uses the facial recognition software.

DIEP Pilot

Contract 359820 – Supplement D authorized additional services for digital image exchange involving Viisage, the AAMVA and the Commonwealth. In particular, this supplement established involvement of all three parties in the Digital Image Exchange Program (DIEP) pilot project. We would ask for answers and supporting documentation for the following questions:

- Q. What is the statutory authority to enter in to this agreement?*
- A. The Department structured the transaction providing for the development of the DIEP to take maximum advantage of the federal funds available to assist the states with the development of secure driver licensing programs. The Secretary of Transportation is empowered by Section 2001.1 of the Administrative Code of 1929, 71 P.S. § 511.1, to enter into contracts as may be necessary to obtain the benefits of federal funding and to carry out the purposes of the Department. Providing for the issuance of a secure driver's license product is clearly a purpose/responsibility of the Department.
- Q. What are the security parameters involved in the DIEP pilot?*
- A. The images and information provided through this program can only be viewed. It cannot be printed or stored. It can only be used to validate a driver's license document presented by the customer. To access the image the requestor must know the state in which the person was licensed and the driver's license number issued by that state. Each request is logged and tracked. Only employees whose job requires them to validate customer identification documents have access to the system.
- Q. Since it is a pilot project, how have any security concerns been addressed regarding new requirements?*
- A. To date, there haven't been any security concerns identified.

Q. Does the AAMVA have access to any driver's license information? If so, what is the statutory authority for allowing AAMVA (a private entity) to view this information?

A. AAMVA provides the network for the exchange of data between states. The data resides at the state level.

Q. What is the statutory authority to allow "digital image exchange standards" to be developed by the AAMVA rather than PennDOT?

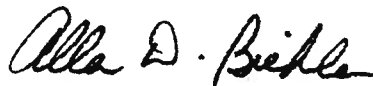
A. By its very definition, a standard is something that shares common aspects. No one state entity could develop a "standard". Understandably, then, there is no statute prohibiting AAMVA from creating a standard.

Q. What standards have been established to date and why?

A. AAMVA has developed technical specifications which allows jurisdictions to perform state-to-state electronic verifications.

As you can see from our responses, PennDOT takes our responsibility to protect customer information seriously. We have developed a comprehensive approach to address security issues. If you have additional questions, do not hesitate to contact Kurt Myers, Deputy Secretary for Safety Administration, at (717) 787-3928.

Sincerely,



Allen D. Biehler, P.E.
Secretary of Transportation

SAMUEL E. ROHRER, MEMBER
128TH LEGISLATIVE DISTRICT
ROOM 45 EAST WING
PO BOX 202128
HARRISBURG, PA 17120-2128
PHONE: (717) 787-8550
FAX: (717) 783-7862
srohrer@pahousegop.com

DISTRICT OFFICE:
29 VILLAGE CENTER DRIVE, SUITE A7
READING, PA 19607
PHONE: (610) 775-5130
FAX: (610) 775-3736
www.samrohrer.com



House of Representatives
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

GAME & FISHERIES,
REPUBLICAN CHAIRMAN
EDUCATION
SPEAKER'S COMMISSION
ON LEGISLATIVE REFORM

CAUCUSES

EAST CENTRAL CAUCUS
PA LEGISLATIVE SPORTSMEN

March 6, 2008

The Honorable Allen D. Biehler, P.E.
Secretary
Department of Transportation
8th Floor
Commonwealth Keystone Building
Harrisburg, PA 17120

Dear Secretary Biehler,

I sincerely appreciate the time and effort involved in your response, dated February 15, 2008, to my questions about Contract 359820 between the Pennsylvania Department of Transportation (PennDOT) and Viisage Technology (Viisage). In particular, the format of your response was very readable and user-friendly.

I had a number of additional questions. In the interest of providing the context for those questions I will adopt the format of your February 15 letter. In other words, I will reproduce the relevant excerpts from the Q and A format of your response and follow with my material and questions. I hope this proves to be a useful means of correspondence. I look forward to your response concerning these additional questions and thank you for your prompt attention to my request.

PennDOT Letter -

- Q.** *What is the accepted human-readable standard in driver's license imaging?*
- A.** AAMVA has published driver license/identification specifications. These specifications were developed by a committee comprised of representatives from various jurisdictions and industry segments for the purpose of assisting states when designing their DL/ID products. These are merely guidelines that jurisdictions can choose to follow if they wish.

The human-readable elements that AAMVA recommends are name, date of birth, gender, driver's license number, address, image, signature, issue date, expiry date, eye color, height, class, endorsements, restrictions, duplicate counter, card type, and jurisdiction name.

- Q. *If this differs from the current standard used by PennDOT, what is the cost difference (computer storage, etc.) between the use of the current standard and the use of a human-readable standard?*
- A. Pennsylvania driver's licenses/identification cards contain all the human-readable data elements recommended by the AAMVA specifications. In addition, it also contains the organ donor designation, when applicable, as required by Act 1994-102.

Additional Questions -

There may have been some confusion about the nature of the questions. These questions focused on the resolution of the photographic images used for a Pennsylvania driver's license. It is my understanding that high-resolution photographic facial images, i.e., images beyond a certain resolution, do not serve to increase the ability of the human eye to distinguish features but do make the photograph more usable for the purposes of facial recognition technology. For example, resolution quality greater than 30 pixels between eye centers may serve this purpose. With that background, I will ask:

- What is the current resolution of photographic images used by PennDOT for driver's licenses?

If the resolution is greater than 30 pixels between eye centers or some other minimum human-readable standard:

- What is the added cost as a result of this upgrade above a minimum standard?
- What is the purpose or intent for obtaining and maintaining an image with this enhanced resolution?

PennDOT Letter -

- Q.** *Who has access to driver's license information maintained by PennDOT, e.g., JNET, other states' departments of motor vehicles, etc.?*
- A.** Pennsylvania law (Section 6114 of Title 75) permits the release of driver's information in the following circumstances:
- Requestor has a signed release of the driver
 - Court order
 - To any Federal, State or local government agency for the sole purpose of exercising a legitimate governmental function or duty.
 - Of a constituent released to a member of Congress or of the General Assembly or to an employee of a member of Congress or of the General Assembly.
 - To a person who, in compliance with the Fair Credit Reporting Act, has filed with the department an affidavit certifying the intended use of said record.
 - To a messenger service which has filed an affidavit of intended use with the department and which maintains on file at its office of record an authorization in writing by the person who is the subject of the obtained record or report.
- Q.** *What is the statutory authority to allow sharing of this information?*
- A.** Section 6114 of the Vehicle Code defines who is entitled to obtain driver information. This Section severely limits those who may have access to the information and the terms and conditions of such access. These are stricter limitations than required by the Federal Driver Privacy Protection Act.

Additional Questions -

This list seems incomplete. According to the terms of Contract 359820, Viisage has access to these records.

- What other private parties have access to these records?
- What is the statutory authority to allow sharing of this information with Viisage and these other private parties?
- The PennDOT letter noted that access is provided to "any Federal, State or local government agency for the sole purpose of exercising a legitimate governmental function or duty." Is this electronic access? Is it granted at will, or does PennDOT make an individual determination for each access based on the merits of the request? Does PennDOT track access by government agencies and maintain a list of these requests? Does PennDOT track access by any of the other parties permitted to obtain information under Section 6114 and maintain a list of these requests?

PennDOT Letter -

Q. *Is this information encrypted?*

A. No. The data contained in the machine-readable technologies (magnetic stripe, two-dimensional barcode, and both one-dimensional barcodes) is not encrypted.

Additional Questions -

- Why is this data unencrypted?
- What protections exist to protect information from capture via card readers in the hands of private entities, etc.?

PennDOT Letter -

Q. *How have all of these issues, including the two aforementioned examples, been addressed by Viisage and PennDOT? Please provide any documentation to supplement answers.*

A. Below is our response for each of the items identified.

Background checks – When PennDOT learned that Viisage had employed individuals prior to the completion of the required background checks, Viisage was instructed to have all background checks completed. Viisage has supplied PennDOT copies of the completed background checks for their employees assigned to the Pennsylvania program. This is not information that can be released.

Additional Question -

- Was there any penalty, contractual or otherwise, for Viisage's security lapse concerning background checks?

PennDOT Letter –

Q. *What is the statutory authority to allow this information to be maintained by a private entity?*

A. AAMVA manages CDLIS. CDLIS was created by the federal "Commercial Motor Vehicle Safety Act of 1986." The Act (49 U.S.C. 321309) required the federal Secretary of Transportation to establish or designate an entity to serve as a clearinghouse for all state jurisdictions. The Secretary designated AAMVAnet as the system operator. Thus, CDLIS is the designated arm of the U.S. Department of Transportation. Providing this information to CDLIS is authorized under Section 6114(b)(4) of the Pennsylvania Vehicle Code and Chapter 95 of the Department's regulations. In addition, federal law now mandates reporting of suspensions, etc., of all drivers to the conjunct National Drivers Register. 49 U.S.C.S. 30304 (2004). These actions are also reported to the

Problem Driver Pointer System (PDPS), consistent with U.S. DOT regulations at 23 CFR 1327.1. Participation in all of these entities is absolutely essential to enable the Department to fulfill the mandates of Pennsylvania law to limit persons to one license (75 Pa. C.S. 1501(c)) and not to license those who are under suspension in another jurisdiction (75 Pa. C.S. 1503(a)(1)).

Additional Questions -

- Has PennDOT had any discussions with AAMVA about participation in the Driver's License Agreement (DLA)?
- If Pennsylvania, through PennDOT, participated in the DLA as it currently exists, would Canada and Mexico have access to Pennsylvania driver's information in the same fashion as other U.S. states?

PennDOT Letter -

- Q. What is the benefit to maintaining driver's license information at private facilities?*
- A.** The Commonwealth has limited technical expertise and resources needed to develop or maintain the equipment and software required to issue photo driver's license/ identification cards. Outsourcing this function is a cost effective solution that has allowed us to improve the security of the issuance process.

Additional Questions -

You noted that this allowed PennDOT to improve security of the issuance process. With that in mind:

- How has this improved security?
- What is the nature of the technical expertise, or what are the resources, that PennDOT does not currently possess?
- What costs would be associated with PennDOT developing the technical expertise and resources "in-house"?

PennDOT Letter -

- Q. What is the statutory authority to engage in the FaceEXPLORER program or similar facial recognition programs?*
- A.** There is no impediment in the law that would prohibit the Department from using this very valuable tool.

Additional Question -

While I appreciate PennDOT's explanation that statutory impediments do not exist, I believe the original question, slightly modified, deserves further exploration.

- What statutory or constitutional authority authorized the Department to take and/or convert images for use as biometric identifiers (e.g., collection of DNA from individuals convicted of felony sex offenses and other specified offenses has been authorized by 44 Pa.C.S. § 2316)?
- What statutory or constitutional authority authorizes expenditures of Commonwealth money and time to create, maintain, control or use the FaceEXPLORER program?

PennDOT Letter -

- Q. *What percentage of current licensing images have been created as, or converted to, facial recognition templates?*
- A. 100 percent of all images.

Additional Questions -

Perhaps it would be useful to have some explanation of the conversion process. In addition to providing information that you believe may be useful for my purposes, I have the following questions:

- What percentage of images were originally recorded in a form used by (or useful for) FaceEXPLORER?
- What percentage of images were converted to this format?
- When did that conversion of images begin?
- How does the conversion process take place, i.e., what needs to be converted or manipulated to make the images useful for FaceEXPLORER or other facial recognition programs?
- Is the quality of converted images the same as images taken today? If not, what is the difference in quality?

PennDOT Letter -

- Q. *What are the uses, currently and those planned for implementation, for FaceEXPLORER and its investigative browser?*
- A. PennDOT currently uses FaceEXPLORER as a tool to help determine if an individual has more than one driver record. The images of all new applicants are compared to all existing images to identify possible matches. In addition, PennDOT is in the process of reviewing all images captured prior to FaceEXPLORER to determine if multiple records exist for one individual. After a comprehensive review has been completed and it

is determined that the individual has more than one record, those driving records are cancelled.

Investigative browser is a fraud prevention tool utilized by the Department's Office of Risk Management and limited law enforcement agencies when conducting an investigation. It provides the ability to take a single image and compare it to all images on the database. This tool allows us to identify someone from their image as well as determine if the individual has established more than one identify.

There are no additional uses planned at this time.

Additional Questions -

- What law enforcement agencies have access to the investigative browser?
- Does this include federal law enforcement agencies?
- Does this include law enforcement agencies from other states?
- Does this include Interpol or any other foreign or international law enforcement agency?
- What types of investigations are conducted using the investigative browser?

PennDOT Letter -

- Q. What controls are in place, including statutory limits on the use of driver's licensing information, to prevent FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?*
- A. Please refer to the question and answer given earlier in reference to how PennDOT uses the facial recognition software.*

Additional Question -

I appreciate PennDOT's explanation of the uses and planned uses of FaceEXPLORER. For the sake of clarity:

- Does PennDOT maintain that there are no statutory limits or other controls in place to prevent the use of FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?

PennDOT Letter -

- Q. Since it (DIEP Pilot) is a pilot project, how have any security concerns been addressed regarding new requirements?*
- A. To date, there haven't been any security concerns identified.*

Additional Questions -

Information which PennDOT provided about the format of the DIEP Pilot is encouraging. I believe, however, that there still may be security concerns when private information (a digital image) is exchanged.

- As the provider of the network for data exchange, does the AAMVA have the ability to access information for testing, quality control or any other purpose?
- If this access for any purpose is allowed, is it tracked in the same way that requests to the system by participants are logged and tracked?

Conclusion

As stated in the opening paragraphs of this letter, I am grateful for PennDOT's serious attention to my inquiries. If you should need any further information, please do not hesitate to contact my office.

Sincerely,



Samuel E. Rohrer
State Representative
128th Legislative District

SER/bjj

cc: Representative Babette Josephs
Representative Gordon R. Denlinger
Representative John J. Siptroth
Representative Thomas E. Yewcic



APR 08 2008

OFFICE OF
SECRETARY OF TRANSPORTATION

COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF TRANSPORTATION
HARRISBURG, PENNSYLVANIA 17101-1900

April 2, 2008

Honorable Samuel E. Rohrer, Member
PA House of Representatives
Room 45 East Wing, Main Capitol
Harrisburg, PA 17120

Dear Mr. Rohrer:

This letter is in response to your correspondence dated March 6, 2008. I have listed your general concerns and each question below with our response.

There may have been some confusion about the nature of the questions. These questions focused on the resolution of the photographic images for a Pennsylvania driver's license. It is my understanding that high-resolution photographic facial images, i.e. images beyond a certain resolution, do not serve to increase the ability of the human eye to distinguish features but do make the photograph more usable for the purposes of facial recognition technology. For example, resolution quality greater than 30 pixels between eye centers may serve this purpose. With that background, I will ask:

Q: What is the current resolution of photographic images used by PennDOT for driver's licenses?

A: Photographic images are being captured at 300 x 360 resolution. The resolution has been in place since the Department implemented its first digital imaging program in 1994. All photographic images have been captured at this resolution.

If the resolution is greater than 30 pixels between eye centers or some other minimum human-readable standard:

Q: What is the added cost as a result of this upgrade above a minimum standard?

A: Sixty pixels of resolution between the eyes is the minimum standard. There is no additional cost to meet this standard.

Q: What is the purpose or intent for obtaining and maintaining an image with this enhanced resolution?

A: This is not an enhanced resolution. This is the minimum standard that was established by PennDOT's first vendor for digital imaging, DataCard, in 1994. Most driver licensing agencies use this same capture resolution or something very similar.

This list seems incomplete. According to the terms of Contract 359820, Viisage has access to these records.

Viisage does not have access to PennDOT's database of driver records. They maintain data that is needed to perform the functions of their contract.

Honorable Samuel E. Rohrer

April 2, 2008

Page 2

Q: What other private parties have access to these records?

A: Access to driver information is only provided to parties who are entitled to receive it under law or are under contract with PennDOT to perform a service on our behalf.

Q: What is the statutory authority to allow sharing of this information with Viisage and these other parties?

A: Third party (including contractor) access to driver record information is subject to Section 6114 of Title 75. As our contractor, Viisage is likewise bound by both Section 6114 and the terms of its contract with regard to disclosure of the driver record information it receives. Depending on the legal authority by which a third party receives driver record information, it is bound by Section 6114, the federal Driver Privacy Protection Act, 18 USC §§ 2721 – 2725 and/or the Fair Credit Reporting Act, as referenced in Section 6114.

The PennDOT letter noted that access is provided to "any Federal, State or local government agency for the sole purpose of exercising a legitimate governmental function or duty."

Q: Is this electronic access?

A: Some government entities have electronic access and others obtain driver information via written requests.

Q: Is it granted at will, or does PennDOT make an individual determination of each access based on the merits of the request?

A: To the extent that law enforcement and other government entities have electronic access, PennDOT does not screen requests on a case-by-case basis. It would be both impractical and possibly even dangerous were we to do so. For example, a State Trooper who has pulled someone over on a remote stretch of highway at 2 a.m. cannot wait for someone from PennDOT to approve the disclosure of driver record information the Trooper needs to know just who it is he or she might be dealing with.

Q: Does PennDOT track access by government agencies and maintain a list of these requests?

A: PennDOT does not maintain a list of each request; however, if an entity obtains information via an online transaction, each request is written to the individual driver's record. If the entity obtains information through a batch process, the request is not recorded on the driver's record, but the entity's input file as well as our output file is maintained for a period of at least three months.

Q: Does PennDOT track access by any of the other parties permitted to obtain information under Section 6114 and maintain a list of these requests?

A: An individual's driving record is annotated each time a request for driver information is made. The driver record is updated to include the date of request, the requestor's name and purpose of request. In addition, PennDOT has the ability to monitor all inquiries made against a driver record.

Q: Why is the data unencrypted?

A: Encrypting the data would eliminate the ability of entities to utilize this technology. The purpose of providing the information on the front of the license in a machine readable format is to allow anyone who currently uses the driver's license/identification card for identification purposes to quickly verify the information is correct.

Q: What protections exist to protect information from capture via card readers in the hands of private entities, etc?

A: It is responsibility of the owner of the driver's license/identification card to protect their data. If they do not want a private entity to have their driver license information, they should not provide them their driver's license. Or, if they choose to provide them their driver's license, they need to take steps to stop them from swiping the card.

Q: Was there any penalty, contractual or otherwise, for Viisage's security lapse concerning background checks?

A: No. The contract does not provide for a penalty or liquidated damages for failure to obtain required background checks. Viisage's transgression, however, was not taken lightly. There were a number of meetings with senior managers of the company, and Viisage was required to obtain the necessary background checks on an expedited basis and provide proof to the Department of those checks under threat of termination of the contract. PennDOT also memorialized Viisage's breach in accordance with Management Directive 215.9 for reference by other Commonwealth agencies potentially considering a contract with the company.

Q: Has PennDOT had any discussions with AAMVA about participation in the Driver's License Agreement (DLA)?

A: PennDOT attended a meeting several years ago sponsored by AAMVA to educate jurisdictions on the proposed requirements of the DLA. PennDOT does plan to attend an informational meeting in late April concerning the DLA.

Q: If Pennsylvania, through PennDOT, participated in the DLA as it currently exists, would Canada and Mexico have access to Pennsylvania driver's information in the same fashion as other U.S. states?

A: Pennsylvania does exchange information (convictions) with Canada and Mexico for commercial drivers via the Commercial Driver License Information System (CDLIS) as required by the federal Motor Carrier Safety Act of 1986. Pennsylvania is not a member of the DLA and, therefore, does not know if the DLA treats Canada and Mexico the same as other states.

You noted that this allowed PennDOT to improve security of the issuance process. With that in mind:

Q: How has this improved security?

A: The process that is in place today allows us to mitigate fraud in a number of ways:

1. When an individual applies for a replacement driver's license/identification card, their image is retrieved, and the product is produced from a central location and mailed to them. This eliminates the possibility of someone stealing another individual's identity.
2. When an individual does not have photo identification in their possession when having their photo taken at time of renewal, their image can be retrieved to verify identity. This technology also reduces the opportunity for identity theft.
3. Utilizing a facial recognition tool (FaceEXPLORER), we are able to compare digital images to reduce the chance of fraud/identity theft.

Q: What is the nature of the technical expertise, or what are the resources, that PennDOT does not currently possess?

A: Viisage, as our Photo License vendor, provides a variety of supplies and services by contract such as hardware, software, product manufacturing, issuance services, inventory control and replenishment, etc. While PennDOT is responsible for issuing driver's license and identification card products to Commonwealth residents, that is only one facet of our core business, which is highway and driver safety. Viisage technology specializes in the issuance of identity and driver license solutions, and that is their core business. Viisage is one of only a very few companies to specialize in this service. Providers of driver's license and ID card credential services, such as Viisage, are experts in product durability, security features, and specialty hardware and software needed to manufacture driver's licenses and identification cards. If this service was not contracted, PennDOT would be responsible for manufacturing items such as specialty cameras, product printers, card stock and security laminate. Additionally PennDOT would need to develop an infrastructure as well as complex computer applications, and provide ongoing support and maintenance for these items. PennDOT would also need to purchase or lease additional facilities to house the equipment, store photo license consumables, house central issuance operations and provide office space for additional staff required to maintain these operations, if located in-house.

Q: What costs would be associated with PennDOT developing the technical expertise and resources "in-house"?

A: Unknown.

While I appreciate PennDOT's explanation that statutory impediments do not exist, I believe the original question, slightly modified, deserves further exploration.

Q: What statutory or constitutional authority authorized the Department to take and/or convert images for use as a biometric identifiers (e.g., collection of DNA from individuals convicted of felony sex offenses and other specified offenses has been authorized by 44 Pa.C.S. § 2316)?

A: Section 1510 of the Vehicle Code requires the Department to include on the license a color photograph or facsimile of the driver. Section 6102 of the Vehicle Code charges the Department with the duty of administering all of the provisions of Title 75. Using reasonable means of detecting license fraud is an absolutely essential function of the administration. Nothing could be more basic to this charge than comparing the photo on one license to the photos on other licenses in order to detect fraud, including identity theft.

Q: What statutory or constitutional authority authorizes expenditures of Commonwealth money and time to create, maintain, control or use the FaceEXPLORER program?

See the answer to the question above. The provisions of the Vehicle Code that charge the Department with the responsibility to administer the provisions of Title 75, assume that the Department will use efficient means to effectuate its duty. FaceEXPLORER creates an economy in detecting potential fraud by allowing one photo to be compared to many others far more quickly than would otherwise be possible.

Perhaps it would be useful to have some explanation of the conversion process. In addition to providing information that you believe may be useful for my purposes, I have the following questions:

Q: What percentage of images were originally recorded in a form used by (or useful for) FaceEXPLORER?

A: Templates have been created for 99.1 percent.

Q: What percentage of images were converted to this format?

A: The images were never converted from their original capture file or formatting parameters. To date, FaceEXPLORER has successfully enrolled and created facial recognition templates for approximately 32.7 million images.

Q: When did that conversion of images begin?

A: Facial recognition template creation began in July 2006.

Q: How does the conversion process take place, i.e., what needs to be converted or manipulated to make the images useful for FaceEXPLORER or other facial recognition programs?

A: There is no conversion of images. To be useful for FaceEXPLORER, images need to be based on the standards defined in ISO/IEC CD 19794-5. In general, FaceEXPLORER works best with these minimum requirements below:

Specification	Value
File format	JPEG or JPEG2000, 256 shades of grey or 24bit color
Compression	10:1 for grey scale, 20:1 for color images
Resolution	240H x 300V x 8 bit grey scale
Eye distance	60 pixels minimum
Position of the eyes, centering	The eyes should be positioned approximately 60-75% of the vertical distance up from the bottom edge of the captured image
Face size	Defined by eye distance (see above)

Q: Is the quality of converted images the same as images taken today? If not, what is the difference in quality?

A: As mentioned above, none of the images have been converted. Photographic images are being captured at 300 x 360 resolution. The resolution has remained the same since the implementation of digital imaging. All photographic images have been captured at this resolution.

Honorable Samuel E. Rohrer
April 2, 2008
Page 6

Q: What law enforcement agencies have access to the investigative browser?

A: Pennsylvania State Police (PSP) and Pennsylvania's Attorney General.

Q: Does this include federal law enforcement agencies?

A: See answer above.

Q: Does this include law enforcement agencies from other states?

A: See answer above.

Q: Does this include Interpol or any other foreign or international law enforcement agency?

A: See answer above.

Q: What types of investigations are conducted using the investigative browser?

A: PSP and Attorney General investigations.

I appreciate PennDOT's explanation of the uses and planned uses of FaceEXPLORER. For the sake of clarity:

Q: Does PennDOT maintain that there are no statutory limits or other controls in place to prevent the use of FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?

A: The Department is not aware of any legal impediment to the potential use of FaceEXPLORER by law enforcement for either surveillance undertaken directly by a law enforcement agency (to the extent that the same was a legitimate function of that particular law enforcement entity) or in conjunction with video from a private system where there is evidence that a crime may have taken place. For instance, if possible, it would be highly beneficial if FaceEXPLORER could be used by police in conjunction with a surveillance photo of a parking lot abduction to detect the identity of a child abductor quickly enough to prevent the child from coming to harm.

Information which PennDOT provided about the format of the DIEP Pilot is encouraging. I believe, however, that there still may be security concerns when private information (a digital image) is exchanged.

Q: As the provider of the network for data exchange, does the AAMVA have the ability to access information for testing, quality control or any other purpose?

A: Per our Memorandum of Understanding with AAMVA, they can only have access to the PA digital image and personal information (name, driver's license number and date of birth) from a PA record, when it has been requested by and permitted by PennDOT.

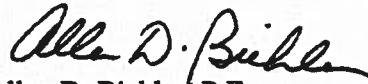
Q: If this access for any purpose is allowed, is it tracked in the same way that requests to the system by participants are logged and tracked.

A: Yes.

Honorable Samuel E. Rohrer
April 2, 2008
Page 7

If you have additional questions, do not hesitate to contact Kurt Myers, Deputy Secretary for Safety Administration, at (717) 787-3928.

Sincerely,

A handwritten signature in cursive script that reads "Allen D. Biehler".

Allen D. Biehler, P.E.
Secretary of Transportation

SAMUEL E. ROHRER, MEMBER
128TH LEGISLATIVE DISTRICT
ROOM 45 EAST WING
PO BOX 202128
HARRISBURG, PA 17120-2128
PHONE: (717) 787-8550
FAX: (717) 783-7862
srohrer@pahousegop.com

DISTRICT OFFICE:
29 VILLAGE CENTER DRIVE, SUITE A7
READING, PA 19607
PHONE: (610) 775-5130
FAX: (610) 775-3736
www.samrohrer.com



House of Representatives
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

GAME & FISHERIES,
REPUBLICAN CHAIRMAN
EDUCATION
SPEAKER'S COMMISSION
ON LEGISLATIVE REFORM

CAUCUSES

EAST CENTRAL CAUCUS
PA LEGISLATIVE SPORTSMEN

May 23, 2008

The Honorable Edward G. Rendell
Governor
Commonwealth of Pennsylvania
225 Main Capitol Building
Harrisburg, Pennsylvania

Dear Governor Rendell,

I am very appreciative of the two responses, dated February 15, 2008 and April 2, 2008, concerning Contract 359820 between Viisage Technology (Viisage) and the Pennsylvania Department of Transportation (PennDOT). It is obvious that PennDOT devoted a significant amount of time and effort to provide answers to my questions.

The terms of Contract 359820, while not officially connected to Pennsylvania's implementation of the REAL ID Act of 2005, raise many of the same constitutional and statutory issues associated with that controversial federal law.

FaceEXPLORER – Lack of Statutory Authorization

While the General Assembly has statutorily authorized the taking of a picture for licensing purposes, we have not statutorily authorized the use of FaceEXPLORER or any similar expansion of the capture or conversion of personally identifiable biometric identifiers. Below are relevant excerpts from both the February 15, 2008 PennDOT letter and the April 2, 2008 PennDOT letter. In both cases, my comments and questions appear in italics and the PennDOT response appears in regular font.

Another concern raised by REAL ID implementation involves the privacy interest in facial images. Specifically, Contract 359820 – Supplement C memorializes an ongoing effort to establish the use of biometric identifiers as part of the Viisage FaceEXPLORER program. The language of Supplement C notes one of the goals of this effort is to "provide capability to create biometric FR templates."

- Q. *What is the statutory authority to engage in the FaceEXPLORER program or similar facial recognition programs?*
- A. There is no impediment in the law that would prohibit the Department from using this very valuable tool.

Q. *How have constitutional issues related to privacy been addressed?*

A. The broad definition of biometrics includes facial recognition. This is a physically non-intrusive technology unlike DNA testing or fingerprinting. PennDOT utilizes facial recognition software as a tool to compare a customer's photograph against our database of photographs to ensure the customer does not have another driver's license issued under a different identity.

PennDOT has determined that the use of this tool is not a constitutional violation. Obtaining a driver's license is a privilege. The state is entitled to condition the grant of that privilege on the individual's consent to have their picture taken and used as necessary to protect security and for other legitimate government functions. It is PennDOT's responsibility to take steps to ensure the integrity of the process, and facial recognition software is one tool we use to do that.

Q. *What controls are in place, including statutory limits on the use of driver's licensing information, to prevent FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?*

A. Please refer to the question and answer given earlier in reference to how PennDOT uses the facial recognition software.

While I appreciate PennDOT's explanation that statutory impediments do not exist, I believe the original question, slightly modified, deserves further exploration.

Q: *What statutory or constitutional authority authorized the Department to take and/or convert images for use as a biometric identifiers (e.g., collection of DNA from individuals convicted of felony sex offenses and other specified offenses has been authorized by 44 Pa.C.S. § 2316)?*

A: Section 1510 of the Vehicle Code requires the Department to include on the license a color photograph or facsimile of the driver. Section 6102 of the Vehicle Code charges the Department with the duty of administering all of the provisions of Title 75. Using reasonable means of detecting license fraud is an absolutely essential function of the administration. Nothing could be more basic to this charge than comparing the photo on one license to the photos on other licenses in order to detect fraud, including identity theft.

Q: *What statutory or constitutional authority authorizes expenditures of Commonwealth money and time to create, maintain, control or use the FaceEXPLORER program?*

See the answer to the question above. The provisions of the Vehicle Code that charge the Department with the responsibility to administer the provisions of Title 75, assume that the Department will use efficient means to effectuate its duty. FaceEXPLORER creates an economy in detecting potential fraud by allowing one photo to be compared to many others far more quickly than would otherwise be possible.

Section 1510 of the Vehicle Code very clearly authorizes PennDOT to obtain a "color photograph or photographic facsimile" of an individual. Section 6102 of the Vehicle Code provides that PennDOT is to "administer" the Vehicle Code. Nothing in these statutory provisions takes the monumental step of permitting PennDOT to create or convert biometric facial recognition templates from the photographic images in its charge.

It is settled law, as explained in the Commonwealth Court's 1997 Mazza opinion, that an "administrative agency is a creature of statute and cannot exercise powers that are not explicitly given to it by the legislature." The court went on to explain that an "agency possesses only those powers conferred to it by statute in clear and unmistakable language." An agency cannot act without statutory authorization, and

the vague, general duties to provide for a system of driver licensing and identification cannot be read so broadly as to allow this foray into a policy with significant constitutional implications. Therefore, from the outset, since PennDOT has not sought authority from the Legislative branch, the conversion of driver license images and the capture of citizens' biometrics in the form of facial recognition technology are in violation of law.

Information Security

In addition to the statutory concerns regarding the use of FaceEXPLORER, I believe there is disagreement about the authority to share these records with Viisage or allow the maintenance of these records by Viisage. It is clear that PennDOT does not have the authority to allow Viisage to have any access to these records under Commonwealth law; and legitimate security breaches by Viisage compound the issues related to private party access to protected information.

Below are relevant excerpts from both the February 15, 2008 PennDOT letter and the April 2, 2008 PennDOT letter. In both cases, my comments and questions appear in italics and the PennDOT response appears in regular font.

- Q. Who has access to driver's license information maintained by PennDOT, e.g., JNET, other states' departments of motor vehicles, etc.?*
- A. Pennsylvania law (Section 6114 of Title 75) permits the release of driver information in the following circumstances:
- Requestor has a signed release of the driver
 - Court order
 - To any Federal, State or local governmental agency for the sole purpose of exercising a legitimate governmental function or duty.
 - Of a constituent released to a member of Congress or of the General Assembly or to an employee of a member of Congress or of the General Assembly.
 - To a person who, in compliance with the Fair Credit Reporting Act, has filed with the department an affidavit certifying the intended use of said record.
 - To a messenger service which has filed an affidavit of intended use with the department and which maintains on file at its office of record an authorization in writing by the person who is the subject of the obtained record or report.
- Q. What is the statutory authority to allow sharing of this information?*
- A. Section 6114 of the Vehicle Code defines who is entitled to obtain driver information. This section severely limits those who may have access to the information and the terms and conditions of such access. These are stricter limitations than required by the Federal Driver Privacy Protection Act.

According to documentation supplied by PennDOT, there are legitimate factual questions about the security performance of Viisage. For example, in October 2001 it appears that Viisage failed to comply with contractual security provisions regarding staff background checks. In 2002, Viisage delivered a shipment of holographic overlays, one of the primary security measures used in the creation of Pennsylvania driver's licenses, to a private business rather than a photo license center.

Q. Have there been other breaches of security protocols by Viisage during the course of any contract with PennDOT? If so, what are the details?

A. In November 2006, the Wilkes-Barre Driver's License Center was burglarized and two computers used to issue driver's licenses were stolen. The thieves also took equipment and supplies that could be used to make fraudulent driver's licenses/identification cards.

During the investigation, PennDOT discovered the computers contained personal information of 11,384 customers who had their photos taken for a driver's license/identification card between August 30, 2006 and November 28, 2006. The information stored on the

computers included names, addresses, dates of birth, driver's license numbers and the last four digits of Social Security numbers. In the case of 5,348 of those customers, the personal information included the complete Social Security numbers. The investigation also revealed that back-up tapes were being stored in an unsecured location. This matter is currently under investigation by the police and the Department is not at liberty to divulge additional information relating to the details of the event.

Q. How have all of these issues, including the two aforementioned examples, been addressed by Viisage and PennDOT? Please provide any documentation to supplement answers.

A. Below is our response for each of the items identified.

Background Checks – When PennDOT learned that Viisage had employed individuals prior to the completion of the required background checks, Viisage was instructed to have all background checks completed. Viisage has supplied PennDOT copies of the completed background checks for their employees assigned to the Pennsylvania program. This is not information that can be released.

Delivery of materials – the incident of holographic overlay being delivered to a private business rather than a photo license center was a failure of UPS. The shipping label used by Viisage clearly states that no indirect delivery can be made. If a delivery issue is identified, it is immediately brought to the attention of UPS management and appropriate disciplinary actions is taken against their employee.

Wilkes-Barre Burglary – PennDOT immediately required Viisage to reduce the time period data remained on the computers as well as encrypt the data. In addition, Viisage was instructed to eliminate the need to store any data for a completed transaction with the planned technology upgrade. The technology upgrade began October 22, 2007 and will be completed statewide by the end of February 2008.

PennDOT placed a stop on all records that were affected to eliminate any fraudulent activity from occurring. New driver's license numbers were issued to the customers whose personal information was contained on the computers. In addition, PennDOT offered free credit monitoring for one year to all individuals impacted.

PennDOT also required Viisage to immediately secure the back-up tapes. They are now kept in a secure facility in Pennsylvania.

Q. Does it provide for the secure destruction of any or all originals or backups under the control of any private entity upon the termination of contract 359820 such that no privately held copies remain in public domain?

A. Contract 359820, Requirement F – Central Image System of RFP, specifies that all files and data are the sole property of the Commonwealth and upon contract termination Viisage must transfer all image files and any custom software required to read the image files to PennDOT.

Sensitive, personal information concerning license Pennsylvania drivers should be maintained under strict and comprehensive security measures. The various documents associated with Contract 359820, which outlines the ongoing relationship between Viisage and PennDOT, discuss the use of Viisage storage facilities to hold private data found in Pennsylvania driver's license records. In the Viisage Proposal of November 1999, there are numerous references to the Central Image System and backup data being held at Viisage, rather than PennDOT, locations. In contract 359820 – Supplement C, there is discussion of moving the backup central image system out of the Commonwealth of Pennsylvania. This is particularly troublesome.

Q. What records of driver's license information, including backup records, are maintained at Viisage facilities or other non-governmental sites?

A. In addition to images and signatures, Viisage's Central Image Server contains all data that is printed on the front of the driver's license/identification card. Viisage also maintains data

on behalf of the Department of State for the Motor Voter Program. For individuals that choose to apply to register to vote through the Photo License Program they maintain county, race, political affiliation and telephone number.

AAMVA manages the Commercial Driver License Information System (CDLIS). CDLIS is a pointer system that contains DL#, name, date of birth, SSN, "AKA" information, and state of record regarding commercial drivers.

Insurance companies get driver record information for their clients or persons seeking to obtain coverage, often through a consumer credit reporting intermediary such as ChoicePoint, under the authority of the Federal Fair Credit Reporting Act. The consumer credit agencies are not allowed to warehouse that data but there is no such similar restriction on the insurance company as the legally authorized end user.

Q. What is the statutory authority to allow this information to be maintained by a private entity?

A. AAMVA manages CDLIS. CDLIS was created by the federal "Commercial Motor Vehicle Safety Act of 1986". The Act (49 U.S.C. 3211309) required the federal Secretary of Transportation to establish or designate an entity to serve as a clearinghouse for all state jurisdictions. The Secretary designated AAMVAnet as the system operator. Thus, CDLIS is the designated arm of the U.S. Department of Transportation. Providing this information to CDLIS is authorized under Section 6114 (b) (4) of the Pennsylvania Vehicle Code and Chapter 95 of the Department regulations. In addition, federal law now mandates reporting of suspensions, etc, of all drivers to the conjunct National Drivers Register. 49 U.S.C.S. 30304 (2004). These actions are also reported to the Problem Driver Pointer System (PDPS), consistent with U.S. DOT regulations at 23 CFR 1327.1. Participation in all of these entities is absolutely essential to enable the Department to fulfill the mandates of Pennsylvania law to limit persons to one license (75 Pa. C. S. 1501 (c)) and not to license those who are under suspension in another jurisdiction. (75 PA. C. S. 1503 (a)(1).)

Q. What is the benefit to maintaining driver's license information at private facilities?

A. The Commonwealth has limited technical expertise and resources needed to develop or maintain the equipment and software required to issue photo driver's license/identification cards. Outsourcing this function is a cost effective solution that has allowed us to improve the security of the issuance process.

Q. Where are those facilities located?

A. The private facility provided under Contract 359820 is located in Pennsylvania. The back-up data is housed in a Commonwealth facility.

Q. Is Viisage allowed to share or provide, with or without a fee, such information to any third party, domestic or international?

A. No. Viisage is prohibited from releasing any information without PennDOT's written approval.

Q. Do any statutory limitations, contractual terms or other protections exist to prevent such sharing of information?

A. Viisage is subject to the restrictions of Section 6114 of the Vehicle Code on the dissemination of driver license information. The Department has enhanced the restrictions in Section 6114 by expressly providing in Viisage's contract that it is prohibited from selling, publishing or distributing the images or data without the written approval of the Commonwealth.

Q: *What is the statutory authority to allow sharing of this information with Viisage and these other parties?*

A: Third party (including contractor) access to driver record information is subject to Section 6114 of Title 75. As our contractor, Viisage is likewise bound by both Section 6114 and the terms of its contract with regard to disclosure of the driver record information it receives. Depending on the legal authority by which a third party receives driver record information, it is bound by Section 6114, the federal Driver Privacy Protection Act, 18 USC §§ 2721-2725 and/or the Fair Credit Reporting Act, as referenced in Section 6114.

Q: *Was there any penalty, contractual or otherwise, for Viisage's security lapse concerning background checks?*

A: No, the contract does not provide for a penalty or liquidated damages for failure to obtain required background checks. Viisage's transgression, however, was not taken lightly. There were a number of meetings with senior managers of the company, and Viisage was required to obtain the necessary background checks on an expedited basis and provide proof to the Department of those checks under threat of termination of the contract. PennDOT also memorialized Viisage's breach in accordance with Management Directive 215.9 for reference by other Commonwealth agencies potentially considering a contract with the company.

PennDOT has cited 75 Pa.C.S. § 6114 in various places as imposing restrictions on access to protected driver's license information. In fact, during our correspondence, PennDOT noted that the protections afforded by Section 6114 are "stricter" than those "required by the Federal Driver Privacy Protection Act."

18 U.S.C. § 2721(a) prohibits any "State department of motor vehicles, and any officer, employee or contractor thereof" from disclosing personal information from motor vehicle records. One of the exceptions to this general rule established in the federal law is that personal information may be disclosed in connection with transportation matters to any "government agency... or any private person or entity acting on behalf of a Federal, State or local agency in carry out its functions." 18 U.S.C. § 2721(b)(1).

While 75 Pa.C.S. § 6114 very clearly allows access to driver's information to any "(f)ederal, State or local governmental agency for the sole purpose of exercising a legitimate governmental function or duty", it does not clearly provide for an exception for private contractors working on behalf of PennDOT. The second sentence of 75 Pa.C.S. § 6114(b)(4), which explains that such "records or reports shall not be resold, published or disclosed by the receiving agency for any commercial purpose nor without prior departmental approval", serves to provide additional limits on republication by a receiving governmental agency and does not expand the original limits provided in the first sentence of that paragraph.

It is understood that both government agencies such as PennDOT and private contractors such as Viisage have the potential to suffer a security lapse. However, if PennDOT is the only entity which maintains these comprehensive records, then the security concern is minimized to the extent that only one entity, rather than two, has the information on hand. Given the past security concerns and the questions concerning statutory authority to share the information, it is suggested that PennDOT investigate retrieval of these records from Viisage and implementation of appropriate means to maintain and secure the information "in-house".

FaceEXPLORER – Constitutional Concerns

In the seminal case of Katz v. United States, it was established that the Fourth Amendment to the United States Constitution protects people rather than places. Subsequent to Katz, there has been case law which has allowed an exception for items exposed to public view, however, this is not dispositive for the purposes of considering PennDOT's use of FaceEXPLORER and the recording/conversion of images for that purpose.

PennDOT is entitled, from both a statutory and constitutional perspective, to capture human-readable facial images for the purpose of driver licensing. But the conversion or use of this image in a biometric modality such as FaceEXPLORER, and in particular that modality's potential for constitutionally suspect use, gives rise to my concerns.

The relevant question is whether an individual has a reasonable expectation of privacy involving the particular facial measurements unique to his or her face. This moves significantly beyond merely capturing an image.

Like many questions involving fundamental privacy rights, it is a matter of degree. Recording the basic, human-readable picture of an individual does not implicate the Fourth Amendment. The "picture" that is exposed to the world, that is, the snapshot appearance of an individual, is not constitutionally protected. In fact, the U.S. District Court for the Eastern District of Pennsylvania recently quoted a portion of the U.S. Supreme Court's Dionisio opinion, which noted,

"No person can...reasonably expect that his face will be a mystery to the world."

The use of FaceEXPLORER is different. It goes beyond merely capturing a picture, or a voice sample, or even a fingerprint, and moves further into the constitutional quagmire created by ever increasing technology. In fact, in more recent decisions such as Kyllo v. United States, the U.S. Supreme Court has indicated some reluctance to embrace new technologies which threaten individual privacy.

In addition to the federal constitutional guarantee, it is also necessary to contemplate the protections of Article I, Section 8 of the Pennsylvania Constitution. In the 2007 Moore case, the Pennsylvania Superior Court quoted its own decision from several years earlier for the proposition that the "notion of privacy implicit in Article I, Section 8 of the Pennsylvania Constitution is particularly strong in this Commonwealth." The court went on to note that "Pennsylvania Courts have recognized that our constitution can provide greater rights and protections to the citizens of this Commonwealth than those provided under similar provisions of the federal constitution." Therefore, independent of the Fourth Amendment to the U.S. Constitution, the language of the Pennsylvania Constitution argues for the privacy of the individual from unwanted and intrusive government action. A 1998 Vermont Supreme Court decision raised questions, under independent state constitutional grounds, about the use of enhanced technology to facilitate video surveillance. Those concerns are similar to the use of enhanced technology which takes a basic picture and converts it to a facial recognition template.

The Fourth Amendment (and corresponding state constitutional) issues related to FaceEXPLORER are compounded by the lack of notice to individuals obtaining a driver's license. Individuals are not on notice that a license picture will be used to create a facial recognition template. Review of the relevant sections of the Transportation Code related to license pictures provides absolutely no notice of this practice since, as aforementioned, it is not statutorily authorized. When an individual is fingerprinted as part of a licensing function, that individual clearly understands the nature of such a procedure and there is a common understanding of how those fingerprints are used. Pictures, on the other hand, are understood as offering a human-readable image rather than a tool to create a facial recognition template.

As part of the exchange between my office and PennDOT, there was discussion about uses for the FaceEXPLORER information gleaned from driver's license images. Beyond using the images to detect individuals attempting to obtain multiple licenses, law enforcement access to FaceEXPLORER compounds the constitutional questions associated with the use of facial recognition technology. This aspect of FaceEXPLORER, and the investigative browser which accesses FaceEXPLORER, was explored in our recent correspondence.

Below are relevant excerpts from both the February 15, 2008 PennDOT letter and the April 2, 2008 PennDOT letter. In both cases, my comments and questions appear in italics and the PennDOT response appears in regular font.

- Q.** *What are the uses, currently and those planned for implementation, for FaceEXPLORER and its investigative browser?*
- A.** PennDOT currently uses FaceEXPLORER as a tool to help determine if an individual has more than one driver record. The images of all new applicants are compared to all existing images to identify possible matches. In addition, PennDOT is in the process of reviewing all images captured prior to FaceEXPLORER to determine if multiple records exist for one individual. After a comprehensive review has been completed and it is determined that the individual has more than one record, those driving records are cancelled.

Investigative browser is a fraud prevention tool utilized by the Department's Office of Risk Management and limited law enforcement agencies when conducting an investigation. It provides the ability to take a single image and compare it to all images on the database. This tool allows us to identify someone from their image as well as determine if the individual has established more than one identity.

There are no additional uses planned at this time.

- Q.** *What controls are in place, including statutory limits on the use of driver's licensing information, to prevent FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?*
- A.** Please refer to the question and answer given earlier in reference to how PennDOT uses the facial recognition software.
- Q:** *What law enforcement agencies have access to the investigative browser?*
- A:** Pennsylvania State Police (PSP) and Pennsylvania's Attorney General.
- Q:** *What types of investigations are conducted using the investigative browser?*
- A:** PSP and Attorney General Investigations.

I appreciate PennDOT's explanation of the uses and planned uses of FaceEXPLORER. For the sake of clarity:

- Q:** *Does PennDOT maintain that there are no statutory limits or other controls in place to prevent the use of FaceEXPLORER (or similar programs) and associated records from being used to implement public surveillance programs tracking the activities of Commonwealth citizens?*
- A:** The Department is not aware of any legal impediment to the potential use of FaceEXPLORER by law enforcement for either surveillance undertaken directly by a law enforcement agency (to the extent that the same was a legitimate function of that particular law enforcement entity) or in conjunction with video from a private system where there is evidence that a crime may have taken place. For instance, if possible, it would be highly beneficial if FaceEXPLORER could be used by police in conjunction with a surveillance photo of a parking lot abduction to detect the identity of a child abductor quickly enough to prevent the child from coming to harm.

While the goal of solving child abduction is a laudable one, its introduction into this particular debate is somewhat distracting. If there are constitutional issues related to law enforcement's access to and use of FaceEXPLORER, then such information could not be used to further criminal prosecution for such an abduction. In fact, the use of constitutionally suspect methods could allow an individual to escape prosecution based on, as expressed in common parlance, a "technicality".

It is worth consideration that the facial recognition templates themselves are testimonial or communicative in nature and therefore inherently subject to a 5th amendment challenge. As noted by the Pennsylvania Superior Court in the Campbell case, "disclosure of one's identity may present self-incrimination issues."

Even beyond those concerns, however, a return to the consideration of the unlawful search and seizure issues associated with this practice would implicate the exclusionary rule and preclude the use of evidence based on this violation.

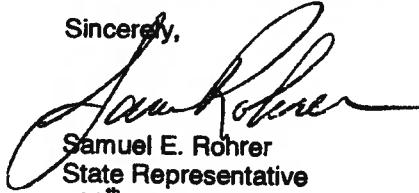
Additional Thoughts and Conclusion

As PennDOT is aware, many of these concerns mirror the legitimate criticisms leveled at interpretations of the REAL ID Act of 2005. Therefore, the current Viisage contract has the potential to exacerbate these problems as the Commonwealth considers if and how to implement the requirements of REAL ID.

It is clear that contracts which violate positive law or are against public policy are unenforceable. It is my contention that various provisions of the current Viisage contract and its amendments fall within one or both of these exceptions to the general rule that contracts will be enforced against a signatory party. I will leave it to PennDOT's judgment concerning whether the contractual agreement with Viisage should be ended or whether the terms could be changed in such a manner as to avoid the statutory, constitutional and public policy issues. These fundamental statutory and constitutional violations demand that the Executive Branch and PennDOT immediately cease any further collection or conversion of biometric data on citizens of the Commonwealth. Further, images currently captured or converted under this biometric paradigm must be reformatted to avoid the significant privacy implications inherent in PennDOT's invasive program.

I am certainly not advocating that PennDOT ignore the potential for fraudulent attempts to obtain multiple drivers' licenses by one individual. To the contrary, there are clearly other effective and less constitutionally suspect means to meet that goal. By reviewing and authenticating birth certificates and other documentary materials, PennDOT will be able to carry on the fight against fraud without such intrusive measures as the use of FaceEXPLORER. I would be happy to talk with PennDOT about the appropriate means and, if necessary, statutory changes to enable this approach. Due to the serious nature of this matter, I will expect a response within seven (7) days.

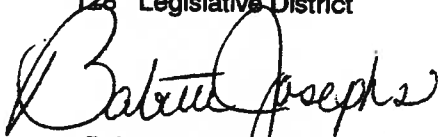
Sincerely,




Samuel E. Rohrer
State Representative
128th Legislative District




John J. Siptroth
State Representative
189th Legislative District



Babette Josephs
State Representative
182nd Legislative District



Thomas E. Yewcic
State Representative
72nd Legislative District



Gordon Denlinger
State Representative
99th Legislative District

SER/bjj

Cc: Allen D. Biehler, P.E.
Secretary of Transportation



COMMONWEALTH OF PENNSYLVANIA
OFFICE OF THE GOVERNOR
HARRISBURG

THE GOVERNOR

June 2, 2008

By Hand Delivery and Fax

**Samuel E. Rohrer, Member
House of Representatives
128th Legislative District
Room 45 East Wing
P.O. Box 202128
Harrisburg, PA 17120-2128**

Re: Viisage Technology – Contract 359820

Dear Representative Rohrer,

I have received your letter dated May 23, 2008 and my staff is working as hard as possible to research the issues you have raised, including determining how other states are resolving these issues.

Thank you for bringing your concerns to our attention. We will respond to your letter in more detail as soon as possible.

Sincerely yours,

A handwritten signature in black ink that reads "Edward G. Rendell".

Edward G. Rendell,
Governor

**cc: Babette Josephs, State Representative
Gordon Denlinger, State Representative
John J. Siptroth, State Representative
Thomas E. Yewcic, State Representative
Steven Crawford, Secretary of Legislative Affairs
Allen D. Biehler, Secretary, Department of Transportation
Barbara Adams, General Counsel**

SAMUEL E. ROHRER, MEMBER
128TH LEGISLATIVE DISTRICT
ROOM 45 EAST WING
PO BOX 202128
HARRISBURG, PA 17120-2128
PHONE: (717) 787-8550
FAX: (717) 783-7862
srohrer@pahousegop.com

DISTRICT OFFICE:
29 VILLAGE CENTER DRIVE, SUITE A7
READING, PA 19607
PHONE: (610) 775-5130
FAX: (610) 775-3736
www.samrohrer.com



House of Representatives
COMMONWEALTH OF PENNSYLVANIA
HARRISBURG

COMMITTEES

GAME & FISHERIES,
REPUBLICAN CHAIRMAN
EDUCATION
SPEAKER'S COMMISSION
ON LEGISLATIVE REFORM

CAUCUSES

EAST CENTRAL CAUCUS
PA LEGISLATIVE SPORTSMEN

June 4, 2008

The Honorable Edward G. Rendell
Governor
Commonwealth of Pennsylvania
225 Main Capitol Building
Harrisburg, Pennsylvania

Dear Governor Rendell,

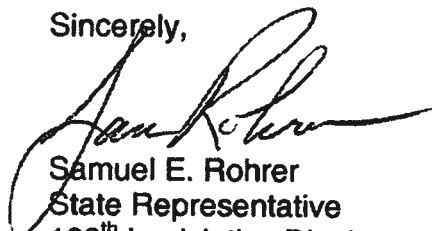
Thank you for your timely response to our letter of May 23, 2008. From your response it appears there may have been some confusion as to the contents of the letter.

While we appreciate your interest in collecting further information from other states, we do not believe that any more facts need to be gathered; nor does there need to be any further investigation concerning the gathering of biometric data by the Department of Transportation. We believe that the facts have already been established.

The thrust of our letter of May 23, 2008 was that the Executive Branch and Department of Transportation immediately cease any further collection or conversion of biometric data on the citizens of the Commonwealth. Further, the Department should convert current database images to a standard which is sufficient for human identification and verification but does not impair the significant privacy and related constitutional interests inextricably linked to the current FaceEXPLORER program.

We would anticipate a response by June 11, 2008 confirming that these concerns have been remedied by the Executive Branch.

Sincerely,


Samuel E. Rohrer
State Representative
128th Legislative District


Babette Josephs
State Representative
182nd Legislative District

June 4, 2008

Page 2



Gordon Denlinger
State Representative
99th Legislative District



John J. Siptroth
State Representative
189th Legislative District



Thomas E. Yewcic
State Representative
72nd Legislative District

SER/bjj

Cc: Allen D. Biehler, P.E.
Secretary of Transportation