Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field

June 30, 2011

Nlets – the International Justice and Public Safety Network

[INSIDE FRONT COVER]

Acknowledgments

Nlets would like to thank the law enforcement practitioners and subject matter experts who volunteered their time, expertise, and experience to create this privacy impact assessment. Without their dedication and willingness to share their wisdom and experience, this document would not be possible.

NLETS FACIAL RECOGNITION WORKGROUP

Jennifer Alkire, Management and Program Analyst
Biometric Center of Excellence
Federal Bureau of Investigation

Sgt. Ronald Critchley, Training Officer
New Jersey State Police

Lt. Kathleen deGrasse, Privacy Officer
Illinois State Police

Sgt. Matthew Joyce, Privacy Officer
New Jersey State Police

Stephen Lamm, Supervisor, ID/Fraud Unit
North Carolina Department of Motor Vehicles

Capt. James Main
Pinellas County Sheriff's Office

Dennis Martin, Management & Program Analyst,
Biometric Center of Excellence
Federal Bureau of Investigation

Michael McDonald, Director, Information Technology Section
Delaware State Police

Lloyd Muenzer, Analyst
Automated Regional Justice Information System

Terry O'Connell, Director, Law Enforcement Data System
Oregon State Police

Roxane Panarella, Privacy Attorney, Office of the General Counsel
Federal Bureau of Investigation

Todd J. Putorti, Sr. Investigator, Division of Field Investigation
New York State Department of Motor Vehicles

Eric J. Radnovich, Director of Justice Services
County of Cumberland, Office of the District Attorney

Mike Robertson, Commissioner
North Carolina Department of Motor Vehicles

Kurt F. Schmid, Executive Director
Chicago High Intensity Drug Trafficking Area

Project leadership and support staff

Bruce Biacar, Department of Homeland Security BAA
Project Sponsor

James Fagan, Department of Homeland Security BAA
Project Sponsor Advisor

George Ake, Sheriff's Association of Texas
Information Led Policing Coordinator

Bonnie Locke, Nlets
BAA Project Director

Frank Minice, Nlets
Chief Technology Officer

Russ Brodie, Nlets
BAA Senior Project Manager

Ted Rainer, Nlets
Project Manager

Wil Nagel
Privacy Consultant

C

Contents

ES

Executive Summary

This report addresses how law enforcement agencies' utilization of facial recognition technologies in the field can impact the public's reasonable expectations of privacy.

There is no uniform set of rules or standards for the use and sharing of information available through facial recognition field identification tools. This lack of regulation can cause the public to fear that they will be automatically identified and their actions monitored by law enforcement agencies through the use of facial recognition systems. Moreover, the potential misuse of facial recognition data may expose agencies participating in such systems to civil liability and negative public perceptions.

The goal of this report is to set forth in a clear and concise manner, the impact facial recognition technologies can have on the public's privacy interests when used to identify people in public. It will also make recommendations for the development of policies and procedures intended to guide departments of motor vehicles and law enforcement agencies' appropriate use of facial recognition technologies in the field.

To assist in the development of this report, Nlets convened a workgroup of practitioners with backgrounds in law enforcement, DMV facial recognition systems, and privacy issues. In their comments on a draft version of this report, several workgroup members stated that this assessment would become an important document when approaching DMVs to participate in a facial recognition field identification tool. The seriousness of the workgroup's discussions reflected the practical experience of the participants, and the results of these deliberations have been incorporated into this report.

HOW INDIVIDUALS WILL BE IDENTIFIED IN THE FIELD

Nlets, the International Justice and Public Safety Network , in cooperation with the U.S. Department of Homeland Security, seeks to develop a set of new data exchanges through which law enforcement officers will be able to access facial recognition software maintained and operated by state departments of motor vehicles to identify individuals in the field.

All state departments of motor vehicles ("DMVs") capture facial images and confirm individuals' biographic information. Furthermore, numerous DMVs currently utilize facial recognition

software to prevent the issuance of fraudulent and duplicative driver licenses and identification cards.

This new capability will enable DMVs to compare facial images collected by law enforcement officers in the field with previously captured driver license and identification card photos. Nlets will provide the data communications network and message protocols for transporting an image captured in the field by a law enforcement officer to a state DMV for submission to its facial recognition software. The facial recognition system will generate a candidate list which will then be returned to the officer over the Nlets network. The entire transaction is expected to take no more than a few minutes.

HOW FACIAL RECOGNITION SYSTEMS WORK

A facial recognition system works in four stages: (1) enrollment; (2) storage; (3) acquisition; and (4) matching. During enrollment, the facial recognition system acquires a facial image and measures distinctive characteristics including but not limited to the distance between the eyes, width of the nose, and the depth of the eye sockets. These characteristics are known as nodal points. Nodal points are extracted from the facial image and are transformed through the use of algorithms into a unique file called a template. A template is a reduced set of data that represents the unique features of the enrolled person's face.

Templates are stored by DMVs for future comparison. To identify people, the facial recognition system compares the biometric template created from a facial with all biometric templates stored in the database. The facial recognition system provides a gallery of potential candidate matches. Human operators can then select the best match from the candidate gallery.

TYPES OF PRIVACY RISKS SURROUNDING THE USE OF FACIAL RECOGNITION TECHNOLOGIES

The public could consider the use of facial recognition in the field as a form of surveillance. The potential harm of surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition. These potential consequences of routine surveillance are often referred to as "chilling effects."

The act of identifying individuals raises privacy concerns because it enables surveillance by facilitating the monitoring of a person. As an instrument of surveillance, identification increases the government's power to control individuals' behavior. It can further inhibit one's ability to be anonymous, which is an important right in a free society.

Interrogation includes various forms of questioning or probing for information. The potential harm associated with the government's gathering of information about people, including their identities, arises from the degree of coerciveness involved. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others.

The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability among those whose information is collected. Moreover, facial recognition systems, in combination with the wide use of video surveillance across the country, would be likely to grow increasingly invasive over time.

The degree of a facial recognition field identification tool's chilling effect depends significantly upon the types of information it collects and how the data will subsequently be utilized. A facial recognition field identification tool will not be a covertly deployed, ubiquitous system utilized to widely identify people without their consent or knowledge. Rather, it will be deployed as a set of standard data exchanges, available for participating law enforcement officials to make discrete inquiries on individuals they have detained.

The chilling effects of a facial recognition field identification tool can be reduced by limiting its use to expressly-stated officer safety and investigatory purposes. Moreover, the collection of long range lens photographs in areas that reasonably reflect an individual's political, religious or social views, associations, or activities can be limited to instances directly related to criminal conduct or activity.

Privacy concerns regarding secondary uses and potential for function creep of facial recognition systems can be addressed by: (1) clearly articulating both the DMV's and law enforcement agency's original purposes for collecting facial images; (2) anticipating and disclosing how facial images are compared by biometric facial recognition systems; and (3) limiting subsequent uses of facial images and comparison matches to the original purposes for which they were collected.

Policies can be developed that set forth the appropriate access and dissemination of facial recognition data; these policies should prohibit and punish individuals who inappropriately disclose facial images obtained from a facial recognition field identification tool. Audits can also be conducted to monitor the use of facial recognition field identification tools. As with other law enforcement data systems, security safeguards should be implemented to limit unauthorized access to facial recognition information.

PURPOSES FOR COLLECTING FACIAL RECOGNITION INFORMATION

Facial images are collected by DMVs and law enforcement agencies for the same purposes: to verify individuals' identities. Knowing an individual's identity allows an officer to ascertain whether the suspect is wanted for another offense or has a record of violence or a recorded mental health disorder. Verifying a person's identity is a necessary element of certain crimes, such as domestic violence cases, and helps officers assess the situation and evaluate any threats to their own safety or possible danger to potential victims.

Collecting and sharing facial recognition information also promotes the strong government interest in solving crimes and bringing offenders to justice. Additionally, establishing an individual's identity can improve a law enforcement agency's efficiency by clearing an individual as a suspect and allowing police to concentrate their efforts elsewhere.

AUTHORITY TO COLLECT FACIAL RECOGNITION INFORMATION

It is axiomatic that law enforcement officers may collect facial images from the general public with their informed consent. Similarly, because people have no reasonable expectation of privacy in facial characteristics that are knowingly exposed in public, long range lens photographs captured by law enforcement officers are also permitted under existing Fourth Amendment jurisprudence.

There is no direct statutory authority requiring individuals to submit to having their facial images captured, however the U.S. Supreme Court has upheld mandatory identification laws that require lawfully detained individuals to identify themselves to police. Thus, states may enact legislation requiring individuals who are lawfully detained to submit to being photographed for identification purposes. In the absence of state law, officers may capture a subject's facial images so long as the individual's identity is related to the investigation of the suspicion that originally justified the detention.

Law enforcement officers also have the authority to capture facial images so long as the detention is reasonably executed and is not prolonged beyond the time necessary to complete the investigation that originally justified the detention. The Driver's Privacy Protection Act and the REAL ID Act both grant DMVs and law enforcement agencies the authority to collect facial images and facial recognition information.

ACCESS TO AND DISSEMINATION OF FACIAL RECOGNITION INFORMATION

Appropriate access to facial recognition information is guided significantly by the purposes for which it was collected. Although state law might impose additional limitations, law enforcement access to DMV facial images returned as part of a facial recognition comparison may be appropriately accessed to: (a) identify individuals driving without a license; (b) identify individuals in possession of a forged or altered driver license or identification card; (c) identify lawfully detained individuals; (d) identify deceased individuals found without identification; (e) identify suspects based upon artists' sketches; (f) identify individuals in surveillance camera footage related to a crime or depicting criminal activity; (g) compile a photo line-up using the suspect's DMV facial image; and (h) identify missing persons who are unable to identify themselves.

It may be appropriate to share DMV facial images with various agencies and individuals throughout the justice system. Any policy regulating the sharing of facial recognition information available via the Nlets network should clearly identify the receiving entity and the specific purpose for the dissemination. Facial recognition information may be shared: (a) among

law enforcement agencies; (b) with other, non-law enforcement government entities; and (c) in certain, limited circumstances with the media and public.

RETENTION OF FACIAL RECOGNITION INFORMATION

The retention of facial images and biometric templates is a matter of policy that should take into consideration, among other things, the justice system's future need for the information as well as the public's reasonable expectations of privacy in the data. A facial recognition field identification tool will not impact how long DMVs retain facial recognition information. There is some tension between a law enforcement agency's need to retain evidence and statutory or regulatory limitations on copying and keeping DMV facial images. Law enforcement agencies should only retain the DMV comparison result gallery where there is an evidentiary or investigative need.

RELIABILITY OF FACIAL RECOGNITION SYSTEMS

Facial recognition systems cannot be 100% accurate. Several issues can impact a facial recognition system's performance; one such issue is variability in the facial images submitted for comparison to the enrolled reference data. Each camera's age, calibration, and compensation for ambient light factors can also result in an individual giving different facial images on different occasions. Despite these issues, facial recognition systems have proven to be valuable tools in identifying people who have applied for or been issued driver licenses or identification cards under multiple names. Requiring trained law enforcement officials to use their judgment in interpreting DMV responses in order to assign or not assign an identity to an individual makes up for potential errors in the automated comparison of facial images.

ACCOUNTABILITY FOR FACIAL RECOGNITION INFORMATION

Many privacy concerns surrounding the use of a facial recognition field identification tool can be mitigated by holding participating agencies accountable for the information they collect and how they subsequently use that information. Existing law enforcement data systems already have policies that include prohibitions against misuse of criminal justice data; those policies also frequently impose penalties for such misuse.

Several methods exist whereby agencies can ensure that their personnel are complying with applicable policies regarding the appropriate collection, use, and dissemination of facial recognition information. Creating tamper-proof audit logs as well as monitoring the use of a facial recognition field identification tool can protect the public's privacy interests. Training authorized users is also a critical accountability measure.

1

Part 1: Overview

Nlets, the International Justice and Public Safety Network, in cooperation with the U.S. Department of Homeland Security, seeks to develop a set of new data exchanges through which law enforcement officers will be able to access facial recognition software maintained and operated by state departments of motor vehicles to identify individuals in the field.

This report addresses how law enforcement agencies' utilization of facial recognition technologies in the field can impact the public's reasonable expectations of privacy. Because agencies interested in accessing facial recognition technologies do not have access to a uniform set of rules or standards for the uses and sharing of information available through facial recognition field identification tools, Nlets has sponsored the preparation of this report.

The goals of this report are two-fold. First, this report sets forth, in a clear and concise manner, the impact facial recognition technologies can have on the public's privacy interests when used to ascertain or verify identities. Second, the report contains recommendations for the development of policies and procedures intended to guide departments of motor vehicles and law enforcement agencies' appropriate use of facial recognition technologies in the field.

A: AGENCIES INVOLVED IN IDENTIFYING INDIVIDUALS IN THE FIELD

Three different types of agencies are involved in helping law enforcement officers verify the identities of the individuals they encounter in the field. Each agency's involvement in the use of facial recognition software as a field identification tool is discussed below.

1: DEPARTMENTS OF MOTOR VEHICLES

There are over 245 million driver license and identification card holders in the United States.[1] All state departments of motor vehicles ("DMVs") currently capture facial images and confirm individuals' biographic information as part of their normal issuance processes.[2] Numerous DMVs are utilizing facial recognition software to prevent the issuance of fraudulent and duplicative driver licenses and identification cards.[3]

[1] Natl. Governors Assn., *The Real ID Act: National Impact Analysis*, 3 (Sept. 2006); Elec. Privacy Info. Center, *REAL ID Implementation Review: Few Benefits, Staggering Costs*, 11 (May 2008).
[2] Natl. Governors Assn. *supra* n. 1 at 11.
[3] *See* Appendix A.

State DMVs will play a critical role in the facial recognition field identification tool. The DMV will conduct the comparison of facial images collected in the field with previously captured driver license and identification card photos. The DMV will then send the comparison results (also referred to as a potential candidate list) back to the officer in the field electronically. Assisting in the identification of individuals furthers DMV missions to promote highway safety and to furnish timely and accurate information to law enforcement officers.

2: LOCAL, STATE, AND FEDERAL LAW ENFORCEMENT AGENCIES

Federal, state, and local law enforcement agencies each have a duty to investigate crimes and criminal conduct. To fulfill this responsibility, police officials identify individuals and collect personally identifiable information about them. A facial recognition field identification tool will give officers the ability to capture a facial image in the field and submit it to specific state DMVs for comparison. The results will help ensure officer safety by establishing the identity of individuals police encounter and investigate.

3: Nlets – the International Justice and Public Safety Network

Nlets will provide the data communications network and message protocols for transporting an image captured in the field by a law enforcement officer to a state DMV for submission to its facial recognition software. Nlets will also transport the results of the DMV's facial recognition comparison search back to the requesting officer in the field.

B: CIRCUMSTANCES GIVING RISE TO CAPTURING FACIAL IMAGES

Essentially, an officer encountering an individual who has no or potentially fraudulent identification will be able to take a digital photograph of the individual's face and submit it, electronically, to a participating state's DMV. The DMV, using its facial recognition system, would then compare the photograph of the individual with the driver's license images stored there and send a potential candidate gallery back to the officer in the field in near real time.

A facial recognition field identification tool can be extremely valuable in situations where ascertaining an individual's identity is an essential element of a crime like domestic violence. The technology could also be useful in identifying individuals to determine whether they are subject to conditions of probation or supervised release. Most importantly, knowing the identity of a suspect allows officers to more accurately evaluate and predict potential dangers that may arise during an investigative stop.[4]

[4] *Hiibel v. The Sixth Judicial District Court of Nevada*, 118 Nev. 868, 874 (2002).

1: HOW POLICE-CITIZEN ENCOUNTERS ARE INITIATED

How an encounter is initiated may have an impact upon whether an officer will capture a facial image to verify an individual's identity. Police-citizen encounters can be initiated by citizens and or the officer and can occur in many contexts. Police-initiated encounters can include, but are not limited to, routine traffic stops and questioning people while walking.[5] Citizen-initiated encounters typically include the following.[6]

1. Reporting a crime;
2. Reporting a traffic accident or medical emergency;
3. Reporting a suspicious person who might be connected to a crime;
4. Reporting suspicious noises;
5. Reporting other events that might lead to a crime;
6. Contacting police about neighborhood concerns or problems;
7. Contacting police to ask for advice or information;
8. Contacting police to give them information; or
9. Reporting any other sort of problem or difficulty.

2: SCENARIOS IN WHICH FACIAL IMAGES MAY BE COLLECTED

There are, generally, five categories of facial images that may be captured in the field by law enforcement officers.[7] These include, but may not be limited to, the following.

First, a facial image may be captured without any types of investigatory detention. These images can be referred to as "long range lens" photographs because they are more likely to be taken from a distance and with less control over environmental conditions that may impact facial recognition comparison. Long range lens photographs may also include surveillance camera footage, photos posted on social networking websites, or sketch artist renderings, provided the images are of sufficient quality.

Second, facial images may be captured during a stop that was not originally justified by reasonable, articulable suspicion as required by the U.S. Supreme Court's decision in *Terry v. Ohio*.[8] These images can be referred to as "unlawful stop" photographs. It is important to note that whether a stop adheres to the requirements of a *Terry* stop is a determination made well after the stop has been concluded.

Third, facial images may be captured during an investigatory stop originally justified by reasonable, articulable suspicion, but the images are not related to

[5] Wesley G. Skogan, *Citizen Satisfaction With Police Encounters*, 8 Police Quarterly 298, 303 (2005).
[6] *Id.*
[7] *See* Molly Bruder, *Say Cheese! Examining the Constitutionality of Photostops*, 57 Am. U.L. Rev. 1693,1702 (2008).
[8] *Terry v. Ohio*, 392 U.S. 1 (1968).

the investigation of the suspicion that originally justified the detention. These images can be referred to as “unrelated investigatory stop” photographs.

Fourth, facial images may be captured during an investigatory stop originally justified by reasonable, articulable suspicion, and the images are related to the investigation of the suspicion that originally justified the detention. These images can be referred to as “related investigatory stop” photographs.

Fifth, a facial image may be captured of an individual in lawful custody who has been placed under arrest. These images are frequently referred to as “mug shots” and it has been long-established that arrested individuals can be required to submit to photographing and fingerprinting for routine identification.[9]

[9] Bruder, *supra* n. 7, at 1705 (*citing inter alia United States v. Amorosa*, 167 F.2d 596, 599 (3d Cir. 1948) (maintaining that photographs obtained lawfully for "routine identification" purposes upon arrest are permissible); *United States v. Kelly*, 55 F.2d 67, 70 (2d Cir. 1932) (upholding fingerprinting upon arrest for identification purposes); and *Illinois v. LaFayette*, 462 U.S. 640, 646 (1983) (explaining that "Inspection of an arrestee's personal property may assist the police in ascertaining or verifying his identity.").

2

Part 2: Fundamentals of Facial Recognition Systems

This part discusses how facial recognition systems function. Specifically, this Part provides a brief overview of how facial recognition systems convert facial images into biometric templates for comparison purposes. This Part also discusses whether facial images and templates should be considered personally identifiable information for purposes of drafting polices and procedures for the use of a facial recognition field identification tool.

A. HOW FACIAL RECOGNITION SYSTEMS WORK

Facial recognition refers to an automated or semi-automated process of matching facial images.[10] Although the term is frequently used as though it refers to a single biometric technology, facial recognition systems all utilize facial images but can rely on different algorithms and biometric scanning technologies.

A biometric indicator is any human physical or biological feature that can be measured and used for the purpose of automated or semi-automated identification.[11] Biometric indicators can be physiological or behavioral.[12] An image of a person's face is a physiological biometric.

Biometrics are used to strongly link a stored identity to the physical person it represents.[13] Because a biometric feature is a part of a person's body, the individual cannot easily separate his registered identity from that feature. Biometric identification works in four stages: (1) enrollment; (2) storage; (3) acquisition; and (4) matching.

During enrollment, the facial recognition system acquires a facial image and measures distinctive characteristics including but not limited to the distance between the eyes, width of the nose, and the depth of the eye sockets. These characteristics are known as nodal points and each human face has multiple nodal points recognizable by facial recognition software. Different software applications may measure different nodal points.

---

[10] Inst. for Prospective Technological Stud., *Biometrics at the Frontiers: Assessing the Impact on Society*, 105 (European Commission Joint Research Centre 2005).
[11] *Id.* at 11.
[12] Natl. Research Council, *Biometric Recognition: Challenges and Opportunities*, 15-18 (2010).
[13] *Id.*

These nodal points are extracted from the facial image and are transformed through the use of algorithms into a unique file called a template. A template is a reduced set of data that represents the unique features of the enrolled person's face.[14] Templates are stored for future comparison.[15]

For identification purposes, the facial recognition system compares the biometric template created from the image captured in the field with all biometric templates stored in the database.[16] For verification purposes, the biometric template of the claimed identity will be retrieved from the database and compared with the biometric template data created from the recently captured facial image.[17]

When an officer in the field requests to identify an individual, the DMV will provide a gallery of potential candidate matches. The law enforcement officer will then select the best match from the candidate gallery.

B. FACIAL RECOGNITION IMAGES AND BIOMETRIC TEMPLATES AS PERSONALLY IDENTIFIABLE INFORMATION ("PII")

Personally Identifiable Information ("PII") is "any information about an individual maintained by an agency, including: (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[18] Although biometric technologies alone do not necessarily link facial recognition to human identity or identification,[19] the National Institute of Standards specifically provides as examples of PII facial images and biometric template data.[20]

There is little doubt that facial images are considered personally identifiable information.[21] Every day, people use faces to identify other people.

---

[14] Inst. for Prospective Technological Stud, *supra* n. 10, at 106.

[15] Essentially the same process is used in the context of fingerprints. *See* Lauren D. Adkins, *Biometrics: Weighing Convenience and National Security Against Your Privacy,* 13 Mich. Telecomm. Tech. L. Rev. 541,542 (2007).

[16] Inst. for Prospective Technological Stud, *supra* n. 10 at 106. This is referred to as a one-to-many (1:N) search.

[17] *Id.* This is a one-to-one (1:1) search.

[18] Erika McCallister, Tim Grance, & Karen Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Special Publication 800-122, 2-1 (U.S. Dept. of Commerce, National Institute of Standards and Technology, April 2010) (adopting a definition of PII used by the U.S. Government Accountability Office).

[19] Natl. Research Council, *supra* n.12, at 22 (explaining that biometric technologies can be employed in anonymous applications).

[20] McCallister, *supra* n. 18, at 2-2.

[21] *See* Driver's Privacy Protection Act, 18 U.S.C. §§ 2725(3); (4) (defining "personal information" as an "individual's photograph, social security number, driver identification number, name, address…telephone number, and medical or disability information" and "highly restricted personal information" as including an "individual's photograph or image, social security number, and medical or disability information"). *See also* Yue Liu, *Identifying Legal Concerns*

Less clear is whether a biometric template alone should be regarded as personally identifiable information.[22] Some authorities consider facial recognition templates as PII because each template is created from the observation of a particular individual and is used primarily to recognize people.[23] Nevertheless, the templates are only useful in the context of a field identification tool when they are attached to a DMV photo. Moreover, the templates will not be transmitted or shared by the DMV. As such, this assessment treats templates as non-personally identifiable information.

in the Biometric Context 3 J. Int'l Com. L. & Tech. 45, 45-46 (2008) (discussing the legal status of raw biometric information under Article 8 of European Union Directive 95/46/EC).

[22] Liu, *supra* n. 21, at 45-46.

[23] *See* Andrzej Drygajlo, head of the Speech Processing and Biometrics Group at the Swiss Federal Institute of Technology at Lausanne, Presentation, *Biometrics* (Sept. 15, 2008) (available on-line at: <http://scgwww.epfl.ch/courses/Biometrics-Lectures-2008-2009-pdf/01-Biometrics-Lecture-Part1-2008-09-15.pdf>).

3

Part 3: Types of Privacy Risks Surrounding the Use of Facial Recognition Technologies

Privacy is a multifaceted concept whose meaning cannot be captured by a crisp and narrow definition.[24] Not only is it multifaceted, but society's reasonable expectations of privacy change as technologies are introduced and become more wide spread.[25] Nevertheless, privacy scholars have attempted to identify precisely each category of privacy harm and describe how the potential harms are related to each other.[26] This Part provides an overview of the major categories of privacy issues implicated by law enforcement officers' use of facial recognition field identification tools.

A: ADDRESSING PRIVACY RISKS – THE FAIR INFORMATION PRACTICES

"The line between technology and the body is blurring."[27] In the context of biometric facial recognition technologies, identities are defined in terms of facial features captured by an algorithm. This means that the image of a person's face has the potential to become a piece of data in need of the same types of protection as other types of personally identifying information.

In 1973, the U.S. Department of Health, Education, and Welfare published a groundbreaking report responding to concerns that harmful consequences may result from the storing of personal information in computer systems. That report, entitled "Records, Computers and the Rights of Citizens," articulated several principles the Department deemed essential to the fair collection, use, storage, and dissemination of

[24] Asimina Vasalou *et al*., Presentation, *The Prototype of Privacy: Analysing Privacy Discourse Through its Features* 2 (British HCI 2010 Conference Privacy and Usability Methods (PUMP) Workshop, Sept. 8, 2010) (available on-line at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1673858>) (outlining 82 privacy features in their proposal to create a dictionary for qualitative researchers).

[25] *See Kyllo v. United States*, 533 U.S. 27, 34 (2001).

[26] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) (articulating a complex taxonomy of privacy problems); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J.___ (forthcoming 2011) (Draft dated July 16, 2010 available online at: <http://papers.ssrn.com/sol3/papers.cfm? abstract_id=1641487>) (advocating the uncoupling of privacy harms from privacy violations and separating privacy harms into objective and subjective categories).

[27] David Lyon, *Identifying Citizens: ID Cards as Surveillance*, 17 (Polity Press, 2009).

personal information by electronic information systems.[28] The report was one of the earliest acknowledgements by the federal government that the public's privacy needed to be protected against arbitrary and abusive record-keeping practices. The report also recognized the need to establish standards of record-keeping practices appropriate for the computer age.

In the intervening years, the fair information practices ("FIPs") have been universally recognized as a solid foundation on which to build privacy legislation and policies.[29] The eight guiding principles evolved from the 1973 report and are frequently used in the analysis and resolution of privacy issues raised by the use of new or advanced information technologies.[30] The principles outlined here play a critical role in addressing the privacy risks that follow.

1: PURPOSE SPECIFICATION PRINCIPLE

The Purpose Specification FIP restricts the uses of information to the reasons for which it was collected. According to this principle, personal information should be collected for specified, explicit, and legitimate purposes and not processed for other purposes.[31] This requires an agency to clearly articulate, no later than at the time the data is captured, the reason for its collection of the information.

2: COLLECTION LIMITATION PRINCIPLE

The Collection Limitation FIP calls on agencies to examine why they collect information in order to avoid collecting information unnecessarily. According to this principle, there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. Limitations on the collection of personal information essentially take two forms: means and relevance.[32]

3: USE LIMITATION PRINCIPLE

Generally, the Use Limitation FIP calls for agencies to limit the use and disclosure of personal information to the purposes articulated in their purpose statements.[33] The principle, however, also provides for four exceptions to this limitation. Specifically,

[28] U.S. Dep't of Health, Educ., & Welfare, *Records, Computers and the Rights of Citizens: Report of The Secretary's Advisory Committee on Automated Personal Data Systems*, xx-xxi (1973) (available at: <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>).

[29] Natl. Crim. Justice Assn., *Justice Information Privacy Guideline*, 22 (2002) (available online at: <http://www.ncja.org/NCJA/Policies_and_Practices/Justice_Information_Privacy_Guideline/NCJA/Navigation/PoliciesPractices/JusticeInformationPrivacyGuideline/Information_Privacy_Guideline.aspx?hkey=d80450ef-9e42-4f05-bb10-1f23222b34ee>).

[30] *See* U.S. Dept. of Homeland Sec., Privacy Office, *Privacy Impact Assessments: The Privacy Office Official Guidance* 18 (June 2010) (referring to the FIPs as Fair Information Practice Principles ("FIPPs")).

[31] Barbara Crutchfield George, *et al*., *U.S. Multinational Employers: Navigating Through the "Safe Harbor" Principles to Comply with the EU Data Privacy Directive*, 38 Am. Bus. L.J. 735, 754 (2001).

[32] Natl. Crim. Justice Assn., *supra* n. 29, at 27.

[33] Natl. Crim. Justice Assn., supra n. 27, at 29.

personal information can be used or disseminated for any reason when: (a) the subject of the data consents; (b) the agency has the legal authority to do so; (c) the safety of the community is at issue; or (d) a public access policy permits the disclosure.[34]

4: DATA QUALITY PRINCIPLE

According to the Data Quality FIP, personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[35]

5: OPENNESS PRINCIPLE

The Openness FIP focuses on the management of the data instead of the actual data itself. Under this principle, there should be a general policy of openness about developments, practices, and policies with respect to personal data.[36] Additionally, means should be readily available of establishing the existence and nature of personal data, and the main purposes of its use, as well as the identity and usual residence of the data controller.

6: INDIVIDUAL PARTICIPATION PRINCIPLE

According to the Individual Participation FIP, an individual should have the right to:[37]

(a) obtain confirmation of whether or not the agency has data relating to him;
(b) Have the data communicated to him in a reasonable time and manner at reasonable cost;
(c) Challenge a denied request under (a) or (b);
(d) Challenge data relating to him and, if successful, have the data erased, rectified, completed or amended with notification to all parties who received the incorrect information; and
(e) Add an annotation to the data where an organization decides not to amend information as requested by the individual.

7: ACCOUNTABILITY PRINCIPLE

Under the Accountability FIP, agencies should have a means of ensuring that their data management policies are followed. Essentially, the principle calls for the development and implementation of due process mechanisms, usually in the form of administrative procedures, through which an individual may challenge an agency's compliance with its privacy policy.[38]

8: SECURITY SAFEGUARDS PRINCIPLE

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. The Security Safeguard principle essentially involves securing privacy through such

[34] *Id.*
[35] *Id.* at 28.
[36] *Id.* at 31.
[37] *Id.* at 32-33.
[38] *Id.* at 33-34.

technologies as encryption, public key infrastructure, digital signatures, role-based access permissions, firewalls, intrusion detection, and virtual private networks.[39]

B. SURVEILLANCE: THE PERCEIVED TRACKING OF INDIVIDUALS

Individuals are already compelled to disclose a great deal of information to their government. For instance, the REAL ID Act, discussed in greater detail in Part 5 of this report, will require individuals to produce documentation of their date of birth, Social Security Number, address of primary residence, and evidence of their lawful status in the U.S. in order to obtain a driver license or identification card they can use to board a commercial airplane.[40]

The public could consider the use of facial recognition in the field as a form of surveillance.[41] At its simplest, surveillance occurs when organizations pay close attention, in routine and systematic ways, to personal data.[42] The potential harm of surveillance comes from its use as a tool of social control. The mere possibility of surveillance has the potential to make people feel extremely uncomfortable, cause people to alter their behavior, and lead to self-censorship and inhibition.[43]

These potential consequences of routine surveillance are often referred to as "chilling effects." Too much social control can adversely impact freedom, creativity, and self-development. Specifically, the risk is that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation because they consider themselves under constant surveillance. Too much social control can also erode the trust model between citizens and the government.[44]

The degree of any biometric system's chilling effect depends significantly upon the types of information it collects and how the data will subsequently be utilized. A facial recognition field identification tool is not a ubiquitous system that is covertly deployed and utilized to identify people without their consent or knowledge. Rather, it will be deployed as a set of standard data exchanges, available for participating law enforcement officials to make discrete inquiries on individuals they have detained. Although the technology can enhance intelligence gathering efforts, it is expected that the vast majority of facial recognition inquiries will take place during traditional police-citizen encounters.

---

[39] *See generally,* IJIS Institute, *Information Security in Integrated Justice Applications: An Introductory Guide for the Practitioner* (February 2003) available at: <http://www.it.ojp.gov/documents/info_fsec_fguide.pdf>.
[40] 6 C.F.R. § 37.11 (2010).
[41] Inst. for Prospective Technological Stud., *supra* n.10, at 10; Natl. Research Council, *supra* n.12, at 90.
[42] Lyon, *supra* n. 27, at 5.
[43] *See* Calo, *supra* n. 26, at 19 (explaining that the perception of being observed doesn't need to be actual as the chilling effects flow from the mere belief that one is being watched).
[44] Institute for Prospective Technological Studies, *supra* n.10, at 68.

Depending upon the quality of surveillance camera footage, photograph, or sketch artist renditions, law enforcement officials may be able to utilize a facial recognition field identification tool to identify suspects. These types of facial images are referred to in Part 1 of this report as long range lens photographs. These situations, which take place outside the traditional police-citizen officer encounter, may enhance the chilling effects of a facial recognition field identification tool. Nevertheless, the development and implementation of policies regulating the capturing of long range lens photographs can reduce these effects.[45] Moreover, the submission of long range lens photographs to DMVs for facial recognition comparison and identification can be limited to the investigation of crimes to reduce the perception that a facial recognition field identification tool is simply a method of public surveillance.[46]

C: IDENTIFICATION: THE EROSION OR COMPROMISE OF ANONYMITY

Identifying individuals is a key theme of twenty-first century life.[47] Identification is the act of connecting data to particular individuals.[48] The act of identifying individuals raises a privacy issue because it enables surveillance by facilitating the monitoring of a person.[49] As an instrument of surveillance, identification increases the government's power to control individuals' behavior.

The potential harm of identification is that it increases the government's power to control individuals through the chilling effects discussed above. It can further inhibit one's ability to be anonymous. The benefits of anonymity in the exercise of First Amendment rights have been recognized by the U.S. Supreme Court. [50] Anonymity is an important right in a free society in so far as it protects people from bias based on their identities and enables people to vote, speak, and associate more freely by protecting them from the danger of reprisal.[51]

The entire purpose of a facial recognition field identification tool is to enhance officer safety by helping law enforcement officials identify the individuals they encounter and investigate. Nevertheless, the chilling effects of identification by a facial recognition field identification tool can be reduced by limiting its use to expressly stated officer

[45] This is an implementation of the Collection Limitation Principle.
[46] This is an effectuation of the Use Limitation Principle operating in conjunction with the Purpose Specification Principle.
[47] Lyon, *supa* n.27, at 4.
[48] Solove, *supra* n. 26, at 511.
[49] *See* Lyon, *supra* n. 27, at 4; 17.
[50] *See NAACP v. Alabama*, 357 U.S. 449 (1958) (reversing a trial court civil contempt order entered against NAACP for failing to disclose membership to the state); *Talley v. California*, 362 U.S. 60 (1960) (reversing a conviction of a Los Angeles ordinance requiring handbills to identify its author and striking down the ordinance as unconstitutional); *Buckley v. American Constitutional Law Foundation* 525 U.S. 182 (1999) (affirming a decision striking down a Colorado requirement for individuals circulating campaign initiative petitions to wear an identification badge).
[51] Solove, *supra* n. 26, at 515.

safety and investigatory purposes.[52] Moreover, the development of policies concerning the collection of long range lens photographs should include provisions concerning the appropriate use of a facial recognition field identification tool in areas known to reflect an individual's political, religious or social views, associations, or activities (e.g., churches, abortion clinics, etc.).[53] In such areas, the collection of long range lens photographs should be limited to instances directly related to criminal conduct or activity.

D: INTERROGATION: THE GATHERING OF IDENTIFYING INFORMATION

Interrogation includes various forms of questioning or probing for information. The potential harm associated with the government's gathering of information about people, including their identities, arises from the degree of coerciveness involved. People often feel some degree of compulsion because not answering might create the impression that they have something to hide. Interrogation forces people to be concerned about how they will explain themselves or how their refusal to answer will appear to others. Historically, interrogation has been employed to impinge upon freedom of association and belief.[54]

Nevertheless, some people may seek to avoid having their photographs taken for a facial recognition system because of concerns about the absence of customary adornments to the face (e.g., scarves, burqa, etc.). Religious beliefs about the body and sectarian jurisdiction over personal characteristics (beards, headscarves) or interpersonal contact (taking photographs, exposing certain parts of the body), may limit the public consensual participation of a facial recognition system.

Identification systems, like driver licenses and facial recognition applications, enhance the government's pursuit of its administrative, economic, political, and public safety goals.[55] Unfortunately, such systems tend to assume that people cannot be trusted to say truthfully who they are and place the burden of proof as to an individual's identity on the identification card.[56]

A facial recognition field identification tool is intended to enhance officer safety by helping law enforcement officials identify individuals they encounter and investigate. The only information collected from individuals is their facial image. Whether a person feels compelled to identify themselves to a police officer has been an issue prior to the advent of facial recognition technologies. At issue is whether individuals will feel coerced into having their photograph taken: (a) to verify that the name provided to the

[52] This is an effectuation of the Use Limitation Principle.
[53] This is an implementation of the Collection Limitation Principle.
[54] Solove, *supra* n. 26, at 501-502.
[55] Lyon, *supra* n. 27, at 69.
[56] *Id.*, at 69-70.

officer is correct; or (b) to identify the individual where they refuse to provide their name.

The degree of coerciveness involved in ascertaining the identity of a person in the field will vary depending upon the nature of the police-citizen encounter. Long range lens photographs do not involve any type of investigatory detention and thus do not involve any coerciveness other than the chilling effects discussed above. The level of coercion present in the capturing of mug shots is not a significant privacy issue because the collection of the facial image is based upon a determination of probable cause.

During the remaining three situations – unlawful stop, unrelated investigatory stop, and related investigatory stop photographs – individuals may feel obligated to submit to having their photograph taken in the field. In some states, lawfully detained persons are required by law to identify themselves to police. Although the level of coerciveness is greater in these states, it is as a result of a legislative enactment.

During a lawful detention, law enforcement officials should be encouraged to ask for an individual's consent to capture a facial image when the individual presents no or potentially fraudulent identification documents. Moreover, policies should include a prohibition on physically stopping people for purposes of capturing a facial image.

E: SECONDARY USE & FUNCTION CREEP: USING THE DATA FOR OTHER PURPOSES

Secondary use is the use of data for purposes unrelated to the purposes for which the data was initially collected without the data subject's consent.[57] The potential privacy harm of secondary use is dignitary in nature in that it can undermine people's reasonable expectations as to the future use of information about them.[58] The potential for secondary use generates fear and uncertainty over how one's information will be used in the future, creating a sense of powerlessness and vulnerability among those whose information is collected.[59]

Facial recognition, in combination with wide use of video surveillance would be likely to grow increasingly invasive over time. Key to the concept of function creep "is that once established, systems can easily acquire an apparent life of their own which is much easier to initiate than to halt or redirect."[60]

The primary goal of a facial recognition field identification tool is to help ensure officer safety by establishing the identity of individuals officers encounter and investigate. The

[57] Solove, *supra* n. 26, at 521.
[58] *Id.*
[59] *Id.* at 522.
[60] Lyon, *supra* n. 27, at 56.

information captured in the field is limited to a facial image and publicly observable demographic information. The results of the inquiry consist of a gallery of potential candidate matches from the state DMV. The law enforcement officer will then select the best match from the candidate gallery.

Privacy concerns regarding secondary uses and potential for function creep of facial recognition systems can be addressed by: (1) clearly articulating both the DMVs and law enforcement agencies original purposes for collecting facial images;[61] (2) anticipating and disclosing how facial images are compared by biometric facial recognition systems;[62] and (3) limiting subsequent uses of facial images and comparison matches to the original purposes for which it was collected.[63]

[61] The Purpose Specification Principle.
[62] The Openness Principle.
[63] The Use Limitation Principle.

4

Part 4: Scope of the Assessment

This part explains the approach this report takes to analyzing and addressing the privacy concerns raised by a law enforcement agency's use of a facial recognition system to identify individuals in the field. It explains the steps taken to prepare this document and decisions related to narrowing the scope of this Privacy Impact Assessment.

A: APPROACH OF THE ASSESSMENT

There is no standard approach for a report of this nature. The analysis conducted in this report is the result of a synthesis of several types of privacy guidance, including, but not limited to: (1) Privacy Impact Assessment guidance developed by several federal agencies as they acted to respond to the E-Government Act of 2002's privacy requirements; (2) the Fair Information Practices developed by Organization of Economic Cooperation and Development to articulate the essential principles for the fair collection, use, and dissemination of personal information by the private sector; and (3) Global Justice Initiative's Privacy and Information Quality Work Group's Privacy Policy Development Guide and Privacy Policy Templates. Essential elements of these sources have been combined to comprehensively address the issues raised by the use of facial recognition systems to identify individuals in the field.

In September 2010, Nlets commissioned the preparation of a privacy impact assessment and a privacy policy in preparation for the development of data exchanges whereby law enforcement officers would be able to access facial recognition software to positively identify individuals in the field. The goal of the privacy impact assessment was to identify and address the primary privacy issues raised by the use of facial recognition field identification tools. To assist in the development of this report, Nlets convened a workgroup of practitioners with backgrounds in law enforcement, DMV facial recognition systems, and privacy issues.

The first step taken in the development of this report was the preparation of a comprehensive listing of privacy challenges confronting the use of a facial recognition field identification tool. On November 15, 2010, workgroup members convened and brought different and complementary perspectives on the listing of privacy issues. The resulting document, entitled *Issue identification: Privacy issues concerning the application of facial recognition technologies to identify subjects in the field via Nlets Data Exchanges* ("the Issues document"), is included in this report as Appendix C.

An initial draft of this report was prepared for review at the December 8, 2010 meeting of the workgroup in Rosemont, Illinois. Participants' comments focused largely upon how DMV facial recognition systems function and how the galleries of potential candidate matches would be presented to law enforcement officers in the field, although many other aspects of the identification tool were thoroughly discussed. Particularly, participants emphasized that no DMV or law enforcement agency was relying completely on a facial recognition system to automatically identify individuals and that a human operator was always utilized to confirm facial recognition system results. Several workgroup members commented that the assessment would be an important document when approaching DMVs to participate in a facial recognition field identification tool. The seriousness of the discussions reflected the practical experience of the participants, and the results of these deliberations have been incorporated into this report.

B: UNDERLYING PREMISES OF THIS REPORT

1: ADULT STATUS IS PRESUMED

States routinely issue driver licenses and identification cards to individuals under the age of majority. Thus, facial images collected by DMVs and law enforcement officers in the field may be of minors. Typically, criminal justice information concerning juveniles is not shared as broadly as the same types of data collected about adults; however, the justifications for limiting access to juvenile justice information may not apply to mere identification. Nevertheless, this report does not discuss facial images collected from adults separately from those collected from minors.

2: EXISTING INFORMATION SHARING PRACTICES REMAIN IN EFFECT

The traditional sharing of investigatory information as a case progresses through the criminal justice system is already the subject of substantial amounts of case law and in some instance court supervision. The discussions contained in this report are not intended to supersede existing data sharing practices concerning the sharing of DMV information with law enforcement agencies.

3: FACIAL IMAGES ON DRIVER LICENSES AND IDENTIFICATION CARDS

In all fifty states, driving is a privilege, not a right. Thus, there is arguably a distinction between a facial image collected as part of a license to drive and a facial image collected for a state identification card. Nevertheless, DMVs routinely treat facial images the same regardless of whether they are collected for a driver license or state identification card. Moreover, the privacy issues outlined in Part 3 of this report are the same regardless of whether the facial image is for a driver license or identification card. As such, this report addresses the privacy impact of using any DMV facial images.

4: FACIAL RECOGNITIONS SYSTEMS UTILIZING MUG SHOTS

It has been long-established that arrested individuals can be required to submit to photographing and fingerprinting for purposes of routine identification. Some law enforcement agencies are utilizing facial recognition systems that can compare submitted facial images with arrest booking photos or mug shots. Many of the overarching privacy issues concerning the chilling effects of surveillance, identification, and function creep still remain in the context of these systems.

Nevertheless, there are fewer statutory restrictions on the use, dissemination, and retention of mug shots as compared to DMV facial images. This is because a mug shot is collected based upon a determination of probable cause that the person committed or was about to commit a crime,

Although this report focuses on facial recognition field identification tools that use DMV images, many of the recommendations can help mitigate privacy risks in the context of facial recognition field identification tools that use mug shots. Even so, law enforcement agencies that utilize facial recognition systems containing mug shots are not required to limit the sharing of their facial images in the same manner as DMVs.

C: ISSUES NOT ADDRESSED IN THIS REPORT

There are numerous privacy and accountability issues surrounding a law enforcement agency's utilization of facial recognition. The scope of this report was narrowed to exclude consideration and discussion of the following issues.

1: DMV COLLECTION OF IDENTIFYING INFORMATION

State and federal laws already address the gathering of identification information that takes place when a person applies for a driver license or identification card from a state DMV. DMV data collection practices are outside the scope of this report.

2: EXCLUSION AND POTENTIAL DISENFRANCHISEMENT OF IDENTIFICATION SYSTEMS

All identification programs involve some ability to sort identified individuals; they are about similarities and differences and about classification and attachment.[64] Today's world increasingly demands proof of legitimate identity in order to exercise freedom.[65] Nevertheless, not everyone has a government issued identification card and those that do possess one may carry the card "with pride, indifference, reluctance, or even fear," depending upon each individuals' personal history and the political conditions of their current or former residence.[66]

Still others may not be able to enroll in a facial recognition system or be recognized by it as a consequence of physical constraints while others may have characteristics that are

[64] Lyon, *supra* n.27, at 40; 67.
[65] *Id.*, at 67.
[66] *Id.*, at 3.

not distinct enough for the facial recognition system to recognize and measure.[67] For example, certain skin tones may cause problems with specific cameras, local lighting, or other environmental conditions.[68] These facts are significant because deployment of identification systems in which certain individuals are consistently unable to participate or can only participate after inconvenient steps, may acquire an unwelcoming reputation no matter how benign the purposes for which it is employed.[69]

While issues surrounding the exclusion and potential disenfranchisement of individuals caused by pervasive identification systems are important, they are much too broad to be addressed within the scope of this report.

3: HEALTH DATA IN FACIAL RECOGNITION SYSTEMS

While the risks of capturing and revealing health-related information are greater with certain biometric technologies (e.g., iris scans and DNA analysis),[70] a facial image can include scars, the aftereffects of illness, and even physical symptoms of drug use. Of the various characteristics used to identify an individual, scars and indicators of chronic diseases are considered unchanging and are therefore more useful for identification purposes.[71]

DMVs already maintain some health-related information regarding drivers and this information will not be included in the Nlets data exchanges that support a facial recognition field identification tool. Thus, this report will not address any health data that may be contained in a facial image nor will laws governing the sharing of health related information be covered.

4: INTELLIGENCE GATHERING USES OF FACIAL RECOGNITION SYSTEMS

A facial recognition field identification tool could be a valuable asset in the collection of criminal intelligence data. For instance, the tool could help identify gang members and their associates through the use of their facial images. As such, intelligence gathering can have a positive impact on officer safety in the field. Nevertheless, intelligence data is already subject to the U.S. Department of Justice's regulations contained at 28 C.F.R. Part 23. Thus, this report focuses on the use of a facial recognition field identification tool during the course of traditional criminal investigations. This report, however, recommends in Part 5 that a facial recognition field identification tool utilize a set of purpose codes so that DMVs can ascertain the reason for each query and make its own determination as to whether such use is in conformance with its state law and policies.

---

[67] Natl. Research Council, *supra* n. 12, at 89.

[68] Inst. for Prospective Technological Stud., *supra* n. 10, at 68; *see also*, Lucas D. Introna & David Wood, *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems* 2 (2/3) Surveillance & Socy. 177, 190 (2004) (explaining a racial bias in facial recognition systems utilizing the Principle Component Analysis (PCA) image template algorithm).

[69] Natl. Research Council, *supra* n. 12, at 90.

[70] Liu, *supra* n. 21, at 45-46.

[71] *Id.*, at 46.

5

Part 5: Collection of Facial Recognition Information

This part explains that facial recognition information essentially consists of captured facial images and the biometric templates created from those images by algorithms. The discussions that follow concern the legal authority to collect facial recognition information and the purposes for which they are collected.

A: TYPES OF INFORMATION COLLECTED

State DMVs collect a substantial amount of information regarding driver license and identification card holders in addition to their facial images. This biographic information is collected to better tie the facial image to an individual. This is sometimes referred to as making people more legible to the government.[72] Facial recognition systems utilize algorithms to create biometric templates from the facial images. It is these templates that are actually compared by the facial recognition software when it compiles a gallery of potential match candidates.

To use a facial recognition field identification tool, law enforcement officers will capture a facial image of someone they encounter or otherwise observe in public. The facial image and publicly observable demographic information will be transmitted over the Nlets network to the DMV.[73]

The DMV's facial recognition system will then create a biometric template from the facial image it receives over the Nlets network. The DMV's facial recognition system will then search the DMV's database for matching templates and compile a gallery of potential candidates. The DMV will then send the gallery containing the facial images of a number of candidates whose templates resemble that of the submitted photo.

The DMV response can rank or sort the candidates' templates based upon how similar they are to the facial image submitted by the officer.[74] DMVs, at their discretion, may restrict their galleries to a limited number of facial images or by only providing images

[72] Lyon, *supra* n. 27, at 22-27.

[73] Collecting and transmitting demographic information such as the individual's gender and/or approximate age narrows the search of facial images and can reduce the impact on DMV facial recognition systems.

[74] Providing actual scores may unduly influence a police officer's decision making process; thus, officers should be trained in how a facial recognition system compiles and ranks a gallery of potential candidate matches. Training is discussed in Part 9 of this report.

that match the submitted template within a certain degree of probability. In instances where multiple DMVs are queried, the response should clearly identify which DMV provided the candidate image and the date on which the image was taken.

B: AUTHORITY TO COLLECT FACIAL RECOGNITION INFORMATION

It is axiomatic that law enforcement officers may collect facial images from the general public with their informed consent. Similarly, because people have no reasonable expectation of privacy in facial characteristics that are knowingly exposed in public,[75] long range lens photographs captured by law enforcement officers are also permitted under existing Fourth Amendment jurisprudence.

While there is no direct statutory authority requiring individuals to submit to having their facial images captured, the U.S. Supreme Court, in *Hiibel v. Sixth Judicial District Court*,[76] upheld mandatory identification laws that require individuals who are lawfully detained during a *Terry* stop to identify themselves to police officers. This decision paves the way for states to enact legislation requiring individuals who are lawfully detained to submit to being photographed for identification purposes. In the meantime, the *Hiibel* decision allows officers to capture "related investigatory stop" photographs so long as the suspect's identity is related to the investigation of the suspicion that originally justified the detention.

There is also legal precedent supporting the premise that law enforcement officers have the authority to capture "unrelated investigatory stop" photographs so long as the detention is reasonably executed and is not prolonged beyond the time necessary to complete the investigation that originally justified the detention.

Finally, the Driver's Privacy Protection Act and the REAL ID Act both grant DMVs and law enforcement agencies the authority to collect facial images and facial recognition information.

A comprehensive discussion of every legal issue associated with the collection of facial recognition information to identify individuals in the field is beyond the scope of this assessment. Nevertheless, an understanding of the broader legal context in which a facial recognition field identification tool will function is important to assessing the technology's impact on individuals' reasonable expectations of privacy.

---

[75] *U.S. v. Dionisio*, 410 U.S. 1, 14 (1973).
[76] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177 (2004).

1: MANDATORY IDENTIFICATION LAWS

Mandatory identification laws, sometimes referred to as "stop and identify" statutes have their roots in early English vagrancy laws.[77] Those laws required suspected vagrants to face arrest unless they provided "a good Account of themselves."[78] Many administrative schemes for identifying individuals were at first partial and were designed to monitor specific segments of the population designated by the fifteenth- and sixteenth-century state system as "suspect."[79] Couriers, for instance, were required to wear special insignia or badges to demonstrate their legitimacy, and beggars in sixteenth-century Cologne and Freiburg were required to register and display badges.[80]

Although in recent decades the Supreme Court has held traditional vagrancy laws void for vagueness,[81] in 2004, the Court upheld a Nevada statute requiring individuals to identify themselves during an investigatory stop permitted by *Terry v. Ohio*.[82]

In *Hiibel v. Sixth Judicial District Court*,[83] a sheriff's deputy was dispatched to a truck stopped on the side of the road to investigate a telephone call reporting an assault between the occupants. When the deputy arrived, he found a man standing by the truck and a young woman sitting inside it. After denying the deputy's requests for identification 11 times, the man was arrested under a Nevada law with having obstructed a police officer by failing to identify himself.

After his arrest, the man was identified as Larry Hiibel. Hiibel was convicted and fined $250.00. He appealed, arguing that the mandatory identification law violated his Fourth and Fifth Amendment rights. The Supreme Court affirmed Hiibel's conviction holding that the request for Hiibel's identity during a *Terry* stop, and Nevada's requirement that he respond, did not contravene the protections of the Fourth and Fifth Amendments. Several portions of the Court's opinion are critical to understanding the legal authority to collect facial images from individuals lawfully detained in the field.

THE EXTENT OF THE IDENTIFICATION REQUIREMENT

The Supreme Court adopted the Nevada Supreme Court's interpretation of the "stop and identify" statute as requiring only that suspects disclose their names; individuals were not necessarily required to produce an ID card or driver's license under the law.[84] This is significant as the Supreme Court previously struck down a California statute that required a suspect to give an officer

[77] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177, 183 (2004).
[78] *Hiibel* at 183. (citation omitted).
[79] David Lyon, *Identifying Citizens: ID Cards as Surveillance*, 20-21 (Polity Press, 2009).
[80] *Lyon supra* n. 79, at 20-21.
[81] *Hiibel supra* n. 77, at 184.
[82] *Terry v. Ohio*, 392 U.S. 1 (1968).
[83] *Hiibel v. Sixth Judicial District Court*, 542 U.S. 177 (2004).
[84] *Hiibel v. Sixth Judicial District Court,* 118 Nev. 868, 875 (2002).

"credible and reliable" identification when asked to identify himself.[85] In the California case, the Court held that the state law requiring "credible and reliable" identification violated the due process clause of the Fourteenth Amendment because it failed to specify what constituted sufficient proof of identification and therefore vested complete discretion in the hands of police officers to either arrest the individual or let them continue on their way.[86] There was no Constitutional infirmity in requiring only that a person state their name to law enforcement officers.

FOURTH AMENDMENT ANALYSIS OF THE IDENTIFICATION REQUIREMENT

In determining that Nevada's "stop and identify" statute was consistent with Fourth Amendment prohibitions against unreasonable searches and seizures, the Court examined what actions a police officer can take during the limited intrusion based upon reasonable suspicion allowed under *Terry.* To ensure a *Terry* stop remains limited, the Court requires an officer's actions to satisfy two requirements: (1) the stop must be "justified at its inception," and (2) the subsequent police actions must be "reasonably related in scope to the circumstances which justified the interference in the first place."[87]

Although it is well established that questions concerning an individual's identity are routine and an accepted part of *Terry* stops, the *Hiibel* case marks the first time the Court has addressed the question of whether a suspect could be arrested and prosecuted for failing to answer.[88] In holding that a person could be arrested and prosecuted for refusing to identify himself to a law enforcement officer, the Court explained that the source of the legal obligation must arise from state law.[89]

The Court also held that the request for identity satisfied the second prong of the *Terry* analysis because it serves important government interests and has "an immediate relation to the purpose, rationale, and practical demands of a *Terry* stop."[90] The Court noted that the Nevada statute did not alter the nature of the stop itself and did not operate to change the duration or location of the detention.

FIFTH AMENDMENT ANALYSIS OF THE IDENTIFICATION REQUIREMENT

The Court held that Nevada's identification requirement did not violate Hiibel's Fifth Amendment rights because he had no reasonable belief that his name would be used to incriminate him or that it "would furnish a link in the chain of

[85] *Kolender v. Lawson*, 461 U.S. 352 (1983).
[86] *Id.* at 358.
[87] *Id.* at 185 (citations omitted).
[88] *Id.* at 186-187.
[89] *Id.* at 187.
[90] *Id.* at 188.

evidence needed to prosecute" him.[91] The Court left open the possibility that Fifth Amendment privilege might apply in a situation where there was a reasonable belief that giving a name could be incriminating, but noted that those situations were likely to be very unusual.[92]

THE EXTENT OF "STOP AND IDENTIFY" LAWS

Currently, 24 states have enacted "stop and identify" laws that require individuals who are lawfully detained to identify themselves.[93] These laws generally require persons who are reasonably suspected of involvement in a crime to identify themselves to the police.[94]

Officers have always been free to look at an individual and compare his likeness to wanted posters and other previously collected mug shots. Although the *Hiibel* case did not directly involve the deputy's use of a biometric technology, the opinion lays the foundation for state legislatures to authorize law enforcement officials to use facial recognition systems.

Unresolved by *Hiibel* is whether the possible loss of privacy posed by automated facial recognition applications is outweighed by improved law enforcement. Nevertheless, many of the privacy issues raised by the intersection of *Hiibel* and biometric technologies can be addressed through reasonable controls over how facial recognition systems are utilized in the field and how the data they capture and create will be managed.

2: ILLINOIS v. CABALLES

Although the Supreme Court suggested in *Hiibel* that an investigative technique (e.g., verifying an individual's identity) must have an "immediate relation" to the circumstances justifying the initial stop, the Court did not apply this standard the following year in *Illinois v. Caballes.*[95] In that case, Roy Caballes was stopped by an Illinois State Police trooper for speeding. A second trooper overheard the radio transmissions concerning the traffic stop and headed to the scene with his drug-detection dog. While the first trooper was preparing the written warning, the second trooper walked his dog around Caballes's car. The dog signaled to the trunk of the car. When the troopers opened the trunk, they found marijuana and arrested Caballes. The entire incident lasted less than 10 minutes.

---

[91] *Id*. at 190.
[92] *Id.* at 190-191.
[93] Appendix B depicts the results of a survey of currently effective stop and identify laws organized by state. Agencies seeking to participate in the facial recognition field identification tool should take steps to determine if their state has a mandatory stop and identify law in effect.
[94] Some states additionally require a suspect to provide police officers with some explanation of his presence and actions. These states are outlined in Appendix B.
[95] *Illinois v. Caballes*, 543 U.S. 405 (2005).

Caballes was convicted of a narcotics offense and sentenced to 12 years' imprisonment and a $256,136 fine. Although the appellate court affirmed, the Illinois Supreme Court reversed the conviction because the use of the drug-detection dog converted the police-citizen encounter "from a lawful traffic stop into a drug investigation" and because the shift in the investigation was not supported by any reasonable suspicion that Caballes possessed drugs.[96] The U.S. Supreme Court vacated the Illinois high court's decision and held that the Fourth Amendment does not require articulable suspicion to justify using a drug-detection dog to sniff a vehicle during a lawful traffic stop.[97]

The Court acknowledged that a seizure that is lawful at its inception can later violate the protections of the Fourth Amendment if the stop and subsequent investigation are conducted in an unreasonable manner.[98] Traffic stops, in particular, can become unlawful if they are prolonged beyond the time reasonably required to complete the written citation or warning.[99] The Court noted that drug-detection dogs are only capable of detecting the presence or absence of contraband. As a result of this limited capability, the Court held that the dog sniff did not implicate legitimate privacy interests where it was conducted during a lawful detention that was not prolonged beyond the time necessary to complete the investigation that originally justified the stop.[100]

Thus, a significant basis of the Court's reasoning was that the sniff of a drug-detection dog was considered unique and did not constitute a search under the Fourth Amendment.[101] Similarly, it could be argued that taking a person's picture in the field and submitting it to a facial recognition system that is only capable of comparing the individual's likeness to the facial images previously stored in it is not a search. Moreover, the use of a facial recognition field identification tool is expected to have no impact upon the duration of the stop. The entire process of capturing a facial image, transmitting it to a state DMV, and receiving the response from the DMV should not take more than a few minutes.[102]

3: DRIVER'S PRIVACY PROTECTION ACT

The Driver's Privacy Protection Act ("DPPA")[103] regulates how state departments of motor vehicles release information contained in their records. The DPPA generally prohibits state departments of motor vehicles from disclosing personal information that their residents submit in order to obtain driver licenses and identification cards.

---

[96] *Id.* at 408.
[97] *Id.* at 407.
[98] *Id.*
[99] *Id.*
[100] *Id.* at 409.
[101] *Id.* at 410-411 (Souter; Ginsburg dissenting).
[102] *See United States v. Place*, 462 U.S. 696, 709-710 (1983) (ruling that a 90-minute delay exceeded the permissible limits of a Terry-type investigative stop), *but see United States v. Sharpe*, 470 U.S. 675, 687-88 (1985) (holding a 20-minute delay reasonable when the police work diligently and where the suspect's actions contribute to some additional delay).
[103] 18 U.S.C.A. §§ 2721-25.

Facial images are contained in the DPPA's definition of "highly restricted personal information."[104] Thus, the DPPA treats facial images collected by DMVs as one of the most protected types of personally identifiable information protected by the law. Nevertheless, the DPPA specifically authorizes DMVs to disclose facial images for use "by any government agency, including any court or law enforcement agency, in carrying out its functions."[105]

The DPPA, in essence, provides a federal baseline of protections for individuals. State legislatures may pass laws to supplement the protections contained in the DPPA, but state law that interferes with or is contrary to federal law is preempted.[106] Therefore, agencies that seek to utilize a facial recognition field identification tool must confirm that their state's law authorizes the collection[107] and sharing[108] of facial images by DMVs.

4: REAL ID Act

The REAL ID Act was passed by Congress in 2005.[109] It requires states to issue driver licenses and identification cards that comply with standards established by the U.S. Department of Homeland Security if those identifying documents will be used to gain access to federal facilities, board federally regulated commercial aircraft, or enter nuclear power plants.

Of particular note, the REAL ID Act requires a facial image be captured for each person *applying for* a driver license or identification card.[110] This differs from existing practices in most states, which currently capture facial images only of those people who are ultimately issued a card.[111] While all states capture facial images as part of the routine issuance process for driver licenses and identification cards, laws in 32 states grant exceptions to the photo requirement for individuals including religious objectors, overseas military personnel, and persons unable to visit a service center due to physical disabilities.[112]

[104] *See* 18 U.S.C.A. § 2725(4). An individual's photograph is also contained in the DPPA's definition of "personal information." *See* § 2725(3). This discussion proceeds on the premise that, by adding the definition of "highly restricted personal information" in 2000 that included facial images, Congress intended for facial images to have the highest level of protection provided for in the DPPA.

[105] 18 U.S.C.A. § 2721(b)(1).

[106] U.S. Const. art. 6, cl. 2.

[107] *See*, e.g., N.H. Rev. Stat. § 260:10-b (providing that "the state shall not collect, obtain, or retain any biometric data in connection with motor vehicle registration or operation, or in connection with driver licensing.").

[108] This issue is addressed in more detail in Nlets Interstate Sharing of Photos (NISP) Project, *Sharing Driver Photos: Privacy Concerns and Mitigation Alternatives* 11-16 (March 10, 2008).

[109] 49 U.S.C. 30301.

[110] 6 C.F.R. § 37.11(a).

[111] Natn'l Governor's Assn., *supra* n. 1, at 11 (explaining that only seven states at that time captured facial images at the beginning of the application process).

[112] *Id.*

The REAL ID act further requires DMVs to make reasonable efforts to ensure that the applicant does not have more than one driver license or identification card already issued by that state under a different identity.[113] Many states are already complying with this requirement through the use of facial recognition systems.[114]

The REAL ID act is not without controversy. Since its passage in 2005, numerous states have passed or considered legislation prohibiting compliance with the federal law.[115] Moreover, pending legislation supported by the U.S. Department of Homeland Security called the Providing for Additional Security in States' Identification Act (PASS Act)[116] would eliminate REAL ID requirements that many states consider excessive and provide federal funding for states to come into compliance.[117] Moreover, the Department of Homeland Security granted all the states an extension of the compliance requirement until May 11, 2011.[118]

Despite the controversy and compliance extensions, the REAL ID act is the currently applicable law. It not only requires the collection of facial images but implicitly authorizes the creation of biometric templates used by facial recognition systems.

C: PURPOSES FOR COLLECTING FACIAL RECOGNITION INFORMATION

The face "is the most common biometric in use by humans to identify other humans."[119] Unlike fingerprints or DNA samples, which are only collected after there is a reasonable level of suspicion of a crime, face images are routinely collected in society by a variety of institutions, such as when we apply for a driver's license, or a passport, or register for classes. Facial images are collected by DMVs and law enforcement agencies for the same purposes: to verify individuals' identities.

Knowing an individual's identity allows an officer to ascertain whether the suspect is wanted for another offense or has a record of violence or a recorded mental health disorder.[120] Verifying a person's identity is a necessary element of certain crimes, such as domestic violence cases, and helps officers assess the situation and evaluate any threats to their own safety or possible danger to potential victims.[121]

---

[113] 6 C.F.R. § 37.13.
[114] *See* Appendix A.
[115] *See* Elec. Priv. Info. Ctr., *REAL ID Implementation Review: Few Benefits, Staggering Costs* 20-21 (May 2008); Cal. Dept. of Motor Vehicles, *Assessment of the REAL ID Act Federal Regulations* 6-4 – 6-6 (April 2008).
[116] Sen. Bill 1261, 111th Cong. (2009).
[117] Spencer S. Hsu, *Administration Plans to Scale Back Real ID Law*, Wash. Post (June 14, 2009).
[118] U.S. Dept. of Homeland Sec., *REAL ID: States Granted Extensions* <http://www.dhs.gov/files/programs/gc_1204567770971.shtm> (November 27, 2010).
[119] Introna & Wood, *supra* n. 68, at 178.
[120] *Hiibel*, *supra* n. 77, at 186.
[121] *Id*.

Collecting and sharing facial recognition information (i.e., facial images and biometric templates) also promotes the strong government interest in solving crimes and bringing offenders to justice.[122] Establishing an individual's identity can also improve efficiency by clearing an individual as a suspect and allowing police to concentrate their efforts elsewhere.[123]

A facial recognition field identification tool can utilize a set of purpose codes so that DMVs can ascertain the reason for each query and make its own determination as to whether such use is in conformance with its state law and internal operating policies. Purpose codes can include but need not be limited to: (a) for traffic stop/officer safety; (b) criminal investigation; (c) intelligence gathering; and (d) government security clearance check.

D: NOTICE CONCERNING THE COLLECTION OF FACIAL RECOGNITION INFORMATION

The most fundamental Fair Information Practice is notice. Without notice, an individual cannot make an informed decision as to whether and to what extent to disclose information to the data collector. Moreover, other fair information practices are only meaningful when a person has notice of an agency's data collection and management practices.

Under the openness principle, agencies should provide notice about how they collect, maintain, and disseminate personal information. Complete notices generally include statements that: (a) describe the main purposes for the data's use; (b) identify the entity responsible for the data; (c) identify those who may access or receive the data; (d) explain whether providing the information is mandatory or voluntary and the consequences of failing to provide the information; and (e) inform the data subject of any rights he may have to access the data and rectify errors.

Just as DMV data collection practices are outside the scope of this report,[124] so too are state DMV notification practices.

The decision to provide the public with notice of a law enforcement agency's use of a facial recognition system involves the consideration of several competing interests. First, there is a growing recognition that promoting public confidence in the administration of justice is one of the primary goals of good government. One way to promote public confidence is to increase the transparency surrounding how facial recognition systems will be managed by the law enforcement agency, even if the facial

[122] *Id*.
[123] *Id*.
[124] *See supra* Part 4: Scope of the Assessment.

recognition information itself should not be released to the public. Doing so serves two purposes: first, it invites constructive comments regarding the operation of the facial recognition system, and second, it is a mechanism to hold the justice system accountable for adhering to the rules and procedures it develops.

There may also be benefits to being proactive about informing the public of the use of facial recognition systems to identify individuals in the field. Since the public is very likely to discover an agency's utilization of the Nlets facial recognition field identification tool, it could be best to be forthcoming with a positive news story.

Nevertheless, there may be drawbacks to providing the public with notice that facial images will be collected in the field and can be submitted to a state DMV for comparison by a facial recognition system. Such notice may add to the controversy surrounding the REAL ID Act. It may also increase public scrutiny of police-citizen interactions. A notice might also inform the public that long range lens photos might also be used to identify people who have not been detained by law enforcement officers.

After weighing the costs and benefits, some agencies may still be interested in providing notice. There are several ways a law enforcement agency can provide the public notice of its use of facial recognition technology to identify individuals in the field. One way is to post a notice on the law enforcement agency's website. To be effective, website notice should be clear and understandable as well as conspicuous and posted in a prominent location.

6

Part 6: Access to and Dissemination of Facial Recognition Information

This part addresses the closely related concepts of access and dissemination of the facial recognition information collected by DMVs and law enforcement agencies.

A: DRIVER DATA AND FACIAL RECOGNITION INFORMATION

This facial recognition field identification tool will rely entirely upon the facial recognition software and databases operated by state DMVs. Facial images captured in the field and transmitted to a state DMV must be enrolled in the state's system for comparison analysis. This is significant because it means that the biometric template created from the facial image remains with the DMV that created it. Additionally, as the facial image captured in the field will not be accompanied by biographical data,[125] a state DMV will not be able to create a record and will not retain the facial image or biometric template after the comparison is complete.

Ultimately, each state's DMV will remain responsible for the operation of its databases and facial recognition software. The facial recognition field identification tool will simply be the vehicle through which law enforcement agencies transmit facial images for comparison and receive the particular DMV's gallery of potential candidates. Thus, the Nlets facial recognition field identification tool only transmits driver license and identification card data that is owned by state DMVs.

B. ACCESS TO FACIAL RECOGNITION INFORMATION

1: DMV ACCESS TO FACIAL IMAGES AND BIOMETRIC TEMPLATES

It is the essential function of state DMVs to collect facial images and create biometric templates for the purposes of comparing facial images. Department of Homeland Security regulations promulgated pursuant to the REAL ID Act specifically provide for a DMV's operation of a facial recognition system to identity instances where individuals have applied for driver licenses and identification cards under multiple names.[126] Moreover, law enforcement agencies routinely provide individuals' PII to DMVs and

[125] A facial image may, however, be accompanied with publicly observable demographic information such as gender and approximate age.

[126] *See* text accompanying *supra* n. 113.

receive, in response, information regarding the subject such as driver license status and past traffic violations. Thus DMVs may also receive facial images from law enforcement agencies for the express purpose of comparing images captured in the field with license and identification card images previously enrolled in the DMV database.

2: LAW ENFORCEMENT ACCESS TO FACIAL IMAGES AND BIOMETRIC TEMPLATES

Law enforcement agencies will not have access to biometric templates via the Nlets facial recognition field identification tool. As discussed above, biometric templates are created by state DMVs as part of the comparison process and are not transmitted from the DMV.

It is axiomatic that law enforcement agencies have access to the facial images they collect and retain. Traditionally, these photos have been in the form of mug shots collected incident to an arrest. Mug shots are typically taken to have a photographic record of the arrested individual to allow for identification by victims and investigators. Mug shots are also collected to ensure the safe-keeping of a prisoner and to prevent his escape, or to assist in the recapture of the prisoner if he should escape.[127] As law enforcement officials begin collecting facial images during detentions, the privacy issue shifts from access to retention.

Law enforcement officials also routinely access state DMV data, but only recently have officers been able to access DMV photos via the Nlets network. The DPPA specifically permits state DMVs to share facial images and personally identifiable information with law enforcement agencies to help carry out its functions.[128] Thus, law enforcement agencies may properly have access to facial images and personally identifiable information of individuals who closely resemble a submitted photograph in an effort to identify the individual.

The only federal limitation on law enforcement access to DMV facial images is that the access must be in furtherance of a law enforcement "function." Although state law might impose additional limitations, access to DMV facial images returned as part of a facial recognition comparison should be permissible in the following instances.

(a) To identify individuals driving without a license;
(b) To identify individuals in possession of a forged or altered driver license or identification card;
(c) To identify individuals lawfully detained as part of a *Terry* stop;
(d) To identify deceased individuals found without identification;
(e) To identify suspects based upon artists' sketches;
(f) To identify individuals in surveillance camera footage related to a crime or depicting criminal activity;

[127] Bruder, *supra* n. 7, at 1705.
[128] *See* text accompanying *supra* n. 105.

(g) To compile a photo line-up using the suspect's DMV facial image;[129] and
(h) To identify missing persons who are unable to identify themselves.

C. DISSEMINATION OF FACIAL RECOGNITION INFORMATION

It may be appropriate to share DMV facial images with various agencies and individuals throughout the justice system. Any policy regulating the sharing of facial recognition information available via the Nlets network should clearly identify the receiving entity and the specific purpose for the dissemination; it should also require audit capabilities.

1: SHARING FACIAL RECOGNITION DATA AMONG LAW ENFORCEMENT AGENCIES

A facial recognition field identification tool is a limited set of message transfers between state DMVs and participating law enforcement officers. Subsequent use of DMV facial images by law enforcement agencies is limited by the DPPA to law enforcement or other government agency functions.[130]

Law enforcement officials have a duty to investigate crimes and criminal conduct. To fulfill this responsibility, officers collect, disseminate, and retain a variety of information, including the identities of individuals who come into contact with officers and those suspected of criminal activity.

As non-matches do not further the law enforcement function of identifying individuals and suspects, law enforcement agencies should be limited to sharing only those DMV facial images that are considered matches.

As a case progresses through the justice system, the identification of an individual should be treated as any other type of evidence in the case. Thus, when necessary to investigate or prosecute a crime, law enforcement officials may share facial images with other law enforcement agencies and prosecutor offices.

2: SHARING FACIAL RECOGNITION DATA WITH OTHER GOVERNMENT ENTITIES

Generally, law enforcement agencies may share DMV facial images obtained via a facial recognition field identification tool with other government agencies so long as the dissemination is to further the receiving or sending agency's function.

---

[129] Most states prohibit the use of individuals' DMV facial images in a photo line-up unless the particular person is suspected of the crime for which the image was requested. *See e.g.*, 92 Ill. Adm. Code 1030.140(b)(3) (providing that "only images of a suspect in the investigation for which the image was requested shall be used in any line-up or photo array.").

[130] 18 U.S.C.A. § 2721(c) (limiting re-disclosure of facial images to those exceptions contained in subsection (b) applicable to "highly restricted personal information.").

3: PUBLIC AND MEDIA ACCESS TO FACIAL RECOGNITION DATA

In response to growing concerns over identity theft and fraud, some privacy advocates suggest that the sharing of any individuals' biometric data be prohibited.[131] Nevertheless, facial images captured in the field and provided by the DMV in response to a facial recognition system inquiry could be useful in preparing photo line-ups[132] and in seeking missing or wanted persons. In these and similar circumstances, law enforcement entities may want to affirmatively distribute facial recognition information to the public.

Generally, DMV facial images may not be shared with the general public, nevertheless a limited release of facial images in furtherance of public safety and law enforcement functions may be permissible. For example, participating law enforcement agencies may wish to share facial images of individuals who pose a threat of harm to the public, are wanted pursuant to a warrant, or missing. A law enforcement agency might also use a suspect's DMV facial image when compiling a photo line-up that can be presented to a victim or other witness for possible identification.[133]

[131] Natl. Research Council, *supra* n. 12, at 51.
[132] *See* text accompanying *supra* n. 129.
[133] *Id.* (explaining that only DMV facial image contained in a photo-lineup would be the suspect's).

7

Part 7: Retention of Facial Recognition Information

The storage of the biometric data is at the center of concern for biometric technology. Although data retention periods were once necessitated by physical storage constraints, electronic storage of records has made the destruction of criminal justice information largely unnecessary. Thus, whether to retain facial images and biometric templates indefinitely is a matter of policy that should take into consideration, among other things, the justice system's future need for the information as well as the public's reasonable expectations of privacy in the data. This part addresses the retention of facial images and comparison results.

A: RETENTION OF FACIAL IMAGES

1: RETENTION BY DMVs

DMVs are solely responsible for the retention of facial images they collect as part of the application for and issuance of driver licenses and identification cards. A facial recognition field identification tool will not impact how long DMVs retain facial images.

2: RETENTION BY LAW ENFORCEMENT AGENCIES

The Fair Information Practices call for the destruction of personal information when it no longer serves its original processing purposes.[134] Typically, once the facial image has been submitted to a state DMV for facial recognition comparison, it has served its original processing purposes. Nevertheless, the facial image collected in the field may take on increased significance if an officer takes investigative steps in reliance upon the DMV information obtained due to the image's submission. As such, law enforcement officers may retain the facial image as part of their investigation records.

Where facial images are gathered as part of an intelligence effort, the retention of the image is governed by the review and purge provisions set forth in 28 CFR § 23.20(h).

[134] This is part of the Use Limitation Principle. *See* George, *supra* n. 31, at 754.

B: RETENTION OF FACIAL TEMPLATES

DMVs are solely responsible for the retention of biometric templates generated from facial images. A facial recognition field identification tool will not impact how DMVs create, compare, or retain biometric templates.

C: RETENTION OF COMPARISON RESULTS

When a law enforcement official submits a facial image for identification, a DMV will respond with a candidate gallery of individuals whose biometric template resembles that of the submitted photograph. Officers in the field will then make a determination as to whether the individual whose identity they seek is one of the candidates provided by the DMV.

As non-matches do not further the law enforcement function of identifying individuals and suspects, law enforcement agencies should consider closely whether they will retain candidate galleries that don't include the subject. There is some tension between a law enforcement agency's need to retain evidence and statutory or regulatory limitations on copying and keeping DMV facial images.[135] Law enforcement agencies should only retain the DMV comparison result gallery where there is an evidentiary or investigative need.

D: RETENTION OF AUDIT LOGS

Nlets will not aggregate or warehouse facial images exchanged between DMVs and law enforcement agencies. Facial images and their associated personally identifiable information will only reside temporarily on the Nlets network during the exchange. A log of the facial recognition inquiry will be maintained by Nlets in a manner consistent with its existing transaction logs. The contents of audit logs are discussed in Part 9 of this report.

[135] *See e.g.,* 92 Ill. Adm. Code 1030.140(a) (prohibiting agencies other than the Illinois Secretary of State from maintaining DMV facial images as part of a database but permitting them to be retained as part of a case record).

8

Part 8: Quality of facial recognition information

A comprehensive discussion of the data quality issues surrounding the use of facial recognition systems is beyond the scope of this report. Instead, this Part introduces the complexities of addressing data quality concerns where facial recognition systems operated by DMVs provide the information that is transmitted electronically to police officers in the field. It concludes that vesting discretion in trained law enforcement officials makes up for potential errors in the automated comparison of facial images and biometric templates.

A. RELIABILITY OF FACIAL RECOGNITION SYSTEMS

Facial recognition systems are "inherently probabilistic and hence inherently fallible."[136] The possibilities of errors (e.g., false positives and false negative identifications) can be made small but cannot be eliminated. Thus, biometric recognition cannot be 100% accurate.[137] Even very small probabilities of error (e.g., the facial recognition system's failure to recognize an enrolled individual or identify an individual as another) can become operationally significant when an application is scaled to handle millions of recognition attempts.[138]

Biometric identification probabilities are only one part of what is necessary to predict the real-world performance of a facial recognition system.[139] In order to accurately express the respective percentages of a facial recognition system's false positive and false negative identifications, the number of individuals who should and should not be identified that are presenting to the system must be quantified.[140] This is extremely difficult, if not impossible, in a DMV setting.

Several issues can impact a facial recognition system's performance; one such issue is variability in the facial images submitted for comparison to the enrolled reference data. In fact, the same individual can provide different facial images at different encounters due to changes in the subject's age, environment, expression, stress, and occupational factors. Each camera's age, calibration, and compensation for ambient light factors can also result in an individual giving different facial images. Better images lead to better

[136] Natl. Research Council, *supra* n.12, at 1.
[137] Drygajlo, *supra* n. 23, at 23.
[138] Natl. Research Council, *supra* n. 12, at 5.
[139] *Id.,* at 37-45.
[140] *Id.*, at 40.

facial recognition results. The matching algorithm utilized by the facial recognition system plays a substantial role in how these variables are handled.[141]

Despite these issues, facial recognition systems have proven to be valuable tools in identifying people who have applied for or been issued driver licenses or identification cards under multiple names. In addition to providing a list of candidates with similar biometric templates, the systems have the ability to score and rank the similarities of the candidates' faces to the facial image submitted for comparison. A facial recognition field identification tool makes this capability available to help officers identify potentially dangerous individuals they encounter during routine stops or persons suspected of criminal activity.

Law enforcement officials should be informed of the limits of the facial recognition technology. For example, officers should understand that facial recognition software is not 100% accurate and that individuals who have a valid driver license or identification card from a DMV might not be recognized by the system every time a picture of the card holder is submitted. With this information, officers must use their judgment in interpreting DMV responses in order to assign, or not assign, an identity to an individual they encounter in the field.

B. INDIVIDUALS' RIGHTS TO ACCESS OR CHALLENGE FACIAL RECOGNITION INFORMATION

The Individual Participation Principle counsels agencies to provide a mechanism for individuals to make inquiries or seek resolution regarding difficulties they experienced as a result of the use of a data system. Nevertheless, the issue of redress is an extremely challenging one in biometric systems and current models of redress may not apply in the context of a facial recognition field identification tool.

It is important to identify precisely which types of information an individual would seek to access or challenge. Essentially, the information exchanged by the facial recognition field identification tool can be distilled to: (1) the facial image collected by the DMV as part of the issuance of driver licenses and identification cards; (2) the facial image captured by the law enforcement official; (3) the biometric templates created by the DMV facial recognition software; and (4) the results of the template comparison search.

Three of the four types of information involved are controlled by a state DMV. Moreover, much of the information collected by DMVs is self-reported by the individual and is supported by appropriate documentation.[142] The last piece of information, the facial image captured by law enforcement officials, is only collected for the purpose of submitting it to a DMV for comparison by its facial recognition system. Thus, it would

[141] *Id.*, at 27.
[142] *See* 6 C.F.R. § 37.13

seem that the agency with the greatest ability to provide any level of access or review would be an individual's state DMV.

In the instance of facial images gathered as part of ongoing investigations, there typically is no comparable right to access or challenge investigative information in the context of the Individual Participation Principle.[143] Any information that Nlets might retain as part of its transaction logs for queries and responses transmitted over its network does not have the potential to create any consequences to individuals that would warrant a need for access and review remedies.

Incorporating the remaining fair information practices into the facial recognition field identification tool policies and procedures may help mitigate the need for any redress procedures, especially where the majority of the data would be in the control of participating state DMVs.

[143] *C.f.,* 28 C.F.R. § 20.3(d) (excluding investigative information from the definition of criminal history record information).

9

Part 9: Accountability for Facial Recognition Information

Many privacy concerns can be mitigated by holding organizations accountable for the information they collect and how they subsequently use that information. Existing law enforcement data systems already have policies that include prohibitions against misuse of criminal justice data; those policies also frequently impose penalties for such misuse. This part describes several methods to verify that participating agencies comply with policies regarding the appropriate use of a facial recognition field identification tool.

A. AUDIT LOGS

Automatically logging transactions involving the sharing of law enforcement information is an effective tool in enforcing access controls and dissemination restrictions. Such logs permit the periodic and random audits necessary to monitor user compliance with relevant laws and policies. Additionally, these logs permit investigations into specific allegations of misuse, unauthorized use, or access to DMV facial images by an unauthorized user. Nlets currently maintains a log of all transactions[144] and will extend this practice to the sharing of DMV facial recognition information.

Transaction audit logs should include at a minimum:

(a) identification of the agency requesting facial recognition;
(b) the purpose code for the facial recognition query;[145]
(c) the date and time the transaction occurred;
(d) header information including the identity of the agency that responded to the inquiry; and
(e) information including a DMV-assigned number and date of image capture that uniquely identifies the facial images transmitted in response to the facial recognition query or a notation that no facial images were available.

Nlets may choose to keep the actual images for audit purposes only. This may prove necessary to provide a complete audit trail for a particular transaction because it is not possible to recreate an exact duplicate candidate gallery by simply re-submitting a facial image through the facial recognition system at a later date. This inability to re-create a transaction is the result of the expanding nature of a DMV database, which enrolls

[144] *See* Sections 8.0.3 and 9.4 of the *Nlets Policies and Procedures*.

[145] A purpose code would be necessary where state law places restrictions on the sharing of DMV facial images in addition to those contained in the DPPA. *See* text accompanying *supra* notes 103 -108.

additional facial images on a daily basis, in addition to the potential differences in facial images captured at different times.[146]

If Nlets retains facial images from DMVs, the images would only be available to Nlets staff for specific audit purposes. Moreover, the audit logs are not designed to be easily searchable and cannot be searched based upon the characteristics of a DMV facial image itself. Audit logs would be searched only in limited circumstances, such as during an investigation of system misuse and when ordered by a court.

B. SECONDARY DISSEMINATION LOGS

The DPPA limits secondary disclosure of DMV facial images to specific uses and requires the creation and maintenance of a dissemination log. Specifically, the DPPA requires any authorized recipient of DMV facial images that re-discloses them, to "keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used."[147] The law further requires that agencies make their dissemination records available to the DMV upon request.[148]

Secondary dissemination logs, like programmatic audit trails, help DMVs monitor the use of their data. When DMV facial images are disseminated outside the law enforcement agency, a log should be maintained that contains: (1) a copy or description of the facial image record disseminated; (2) the date and time the information was disseminated; (3) the identity of the individual to whom the information was released, including their agency and contact information; and (4) the purpose for which the facial image will subsequently be used.

C. MONITORING AND CONDUCTING AUDITS OF SYSTEM USE

As with any data system, a facial recognition field identification tool carries with it the potential for abuse.[149] Monitoring and conducting audits of the facial recognition field identification tool can help to verify that participating agencies are operating in accordance with applicable laws, regulations, and Nlets policies.

An audit of the facial recognition field identification tool would involve an evaluation of a law enforcement agency's utilization of the application and the facial recognition information the agency received from state DMVs. Such audits could focus on: (1)

---

[146] Part 8(A) discusses some of the reasons why the same individual might provide different facial images at different encounters.

[147] 18 U.S.C. § 2721(c).

[148] *Id.*

[149] *See* ACLU, *Q&A On Face-Recognition* <http://www.aclu.org/technology-and-liberty/qa-face-recognition> (last updated Sept. 2, 2003) (Accessed on Dec. 1, 2010).

determining whether facial images are appropriately captured in the field; (2) confirming that DMV facial images are only disclosed to authorized individuals and agencies; and (3) limiting the utilization of the facial recognition field identification tool for official law enforcement purposes only. To accomplish this task, auditors should be familiar with common misuses of facial recognition applications and the comparison search results produced by the DMV software.

Existing law enforcement data systems already have policies that include prohibitions against misuse of criminal justice data; those policies also frequently impose penalties for such misuse.[150] These existing policies may be incorporated into information management policies guarding against misuse of a facial recognition field identification tool.

D. POLICY AWARENESS AND TRAINING

Law enforcement officials utilizing a facial recognition field identification tool must be trained to recognize when they can and cannot capture a facial image for submission to a state DMV for comparison. Law enforcement officers should also be made aware of the reasons why policies limiting the use of the facial recognition field identification tool exist and how those policies protect their agency and the public. Educating users on the proper use of facial recognition systems and DMV facial images is a continual process that must be regularly updated as laws and regulations governing biometric data systems and DMV data change.

Each participating law enforcement agency will have the responsibility of ensuring that its personnel have completed training about the appropriate use and sharing of information obtained from a facial recognition field identification tool. Policies regarding the use of a facial recognition field identification tool and the DMV facial images transmitted over the network should be easily accessible by law enforcement officers and, depending upon the level of detail, available to the public as well. Authorized users should be informed about how facial recognition policies will be enforced, including any penalties for committing violations of the policy provisions.

This facial recognition solution is only a tool for the officer to use. Officers utilizing the facial recognition field identification tool should also be trained how to interpret the facial recognition results. It is the responsibility of the officer to evaluate the DMV facial recognition results along with other available identifying information to make the best determination possible as to a subject's identity.

[150] The report treats DMV facial images released pursuant to the law enforcement exception of the DPPA, 18 U.S.C.A. § 2721(b)(1), as criminal justice data.

E. SECURITY SAFEGUARDS

Security safeguards are another way of ensuring that facial recognition information is accessed only by those authorized to receive it. As such, the transmission of facial recognition information over the Nlets network should be secure from both external and insider threats, whether physical or cyber in nature. Moreover, the facial images should also be encrypted during transmission across the Nlets network to prevent unauthorized access and accidental disclosure. Ensuring that the facial images and DMV facial comparison results remain secure is a vital component of the trust model between citizens and their government.

Law enforcement agencies should also take steps to help secure facial recognition information accessed over the Nlets network. In particular, agency computing devices that access facial images should utilize anti-virus software and firewalls. Role-based user IDs and alphanumeric passwords consisting of a combination of upper and lower case letters, numbers and symbols should also be utilized to access agency data systems. Law enforcement agencies should also utilize encryption technologies to protect the DMV facial images they re-disclose over other electronic networks.

A

Appendix A: Use of Facial Recognition Technology by State

In the first half of 2011 a state survey of Facial Recognition Technologies was performed. State Nlets representatives were contacted and request they respond to a set of questions regarding their use of Facial Recognition Technologies. The following statements requested their input:

> Nlets is currently developing a Privacy Impact Assessment (PIA) for the use of Facial Recognition System (FRS) technology for state driver license image verification. The goal is to provide a comprehensive foundation for states to modify and/or enhance their statutes to enhance officer and citizen safety.
>
> Development of effective and solid policies enables officers to send photos via a cell phone or other devices, via the secure Nlets network, to a specific state DMV where automated facial recognition will be performed and returned in real-time. Once developed, the PIA and supporting policies and procedures will be made available to each Nlets representatives thus helping field officers identify individuals.

The following questions were included on the survey:

1. Does any agency in your State utilize Facial Recognition System (FRS) Technology?
2. To your knowledge does any agency of “state government” intend to deploy FRS Technology by the end of 2011?
3. Please list all “state government” agency(s) utilizing Facial Recognition Systems.
4. Please list all the purposes for which FRS is being utilized in your State.
5. Is your state in compliance with the REAL ID Act?
6. Has your State publicly stated it refuses to comply with the REAL ID Act?
7. Please add any information you believe is relevant and/or interesting as it relates to FRS Technology.

Note: For information about the FBI's Facial Identification Scientific Working Group (FISWG) visit website: http://www.fiswg.org

State	1. Any Agency utilizing FRS	2. Intend to deploy FRS in 2011	3. Agencies utilizing FRS	4. Purpose of FRS	5. Compliance with REAL ID	6. Refuse to comply with Real ID	7. Relevant and/or interesting information relating to FRS
Alabama	No	No					
Arkansas	Yes		Used by the Arkansas Office of Driver Services, also the Arkansas Crime Information Center is a user of the Driver Services system.	Prevention of driver license fraud. Assisting law enforcement in identification of suspects.	No	No	
Colorado	No	No					The State has discussed the prospect in using it for comparison of DMV photos to mug shots but we are still waiting to implement the DMV photo transfer. There has been nothing concrete at this time.
Connecticut	Yes		Used by the CT Department of Motor Vehicles (CT DMV) Document Integrity Unit.	Reduce the incidence of multiple identification credentials issued to the same person. Through CTIC (Connecticut Intelligence Center) CT DMV will assist law enforcement in identification of suspects.	Yes		Since CT DMV began to use FR in 1996, 8,500 credentials have been revoked based on FR identification of multiple identities.
District of Columbia	No	No					
Florida	Yes		Numerous agencies use this capability including: Department of Highway Safety and Motor Vehicles DHSMV, Department of Corrections, DC Pinellas County Sheriff, Miami-Dade Police Department and many others	Fraud, Investigations, Identity Confirmation, Booking, etc.	Yes		Florida is a charter member on the Facial Identification Scientific Working Group (FISWG) -- www.fiswg.org -- which is sponsored by the FBI's Biometric Center of Excellence FDLE is currently the Chair for Collection, Transmission and Storage Subcommittee for FISWG.
Guam	No	No					It would be beneficial for our local government to have this ability.
Hawaii	No	Yes					The State is currently looking to procure Morpho Face Investigate (MFI) as the State has MorphoTrak for its AFIS. The plan is to use in supporting the APEC conference in November. Limiting factors are funding, time for addressing issues (e.g. PIA, statutes, implementation, etc.).

State	1. Any Agency utilizing FRS	2. Intend to deploy FRS in 2011	3. Agencies utilizing FRS	4. Purpose of FRS	5. Compliance with REAL ID	6. Refuse to comply with Real ID	7. Relevant and/or interesting information relating to FRS
Illinois	Yes		Illinois Secretary of State's Office uses FRS in the Drivers License process. Illinois State Police uses FRS for the Firearms Owners Identification (FOID)System. It is used as a validation step to ensure the person being issued a FOID card is the person they claim to be. There are other classified uses as well.	Fraud detection for DL and FOID Card; Identification of Suspects on a limited basis.	Unknown		What is the success and viability of systems that use FRS to scan crowds or moving lines to identify subjects/suspects? What privacy concerns have been raised, and is there case law in support or opposition to FRS? Are there alternative technologies to FRS that are emerging that may prove either more effective, or more efficient for the future? What is the experience of utilizing FRS on a mobile device such as a BB, I-phone, or Android?
Indiana	Yes		Currently only our Bureau of Motor Vehicles	Reduce multiple issuance	Yes		Fusion center is looking at this technology.
Kansas	Yes		Used by the Department of Motor Vehicles.	DMV uses to reduce issuance of multiple ID cards	Unknown		
Kentucky	Yes		Used by the Kentucky State Police	Mostly for comparison of photos to the Driver's License database for purpose of identification	No	Unknown	Experience with FRS is that unless conditions are sterile, they are largely useless. For example, unless a photo of a suspect/missing person, etc., is at an angle identical to the DMV photos on file (with similar lighting and facial expression), the chances of a match are slim.
Louisiana	No	No					
Maine	No	No					
Maryland	Yes		Used by the Department of Public Safety and Corrections to provide a tool to the Criminal Justice community in Maryland.	Criminal Justice agencies use this for investigation and identifications	No	No	
Minnesota	Yes		Used by the Department of Public Safety Bureau of Criminal Apprehension (BCA) and the Department of Public Safety Driver Vehicle Services (DVS) (Pilot Project)	BCA/LE Investigative purposes, DVS Detect Fraud	Unknown		
Mississippi	Yes		Used by the Driver Services Division of MS Dept of Public Safety	Driver Services utilizes the FRS to detect multiple identification cards issued to the same individual. Driver Services also supports law enforcement by using FRS to search for matches to a suspect.	Yes		MS presently has no automated interfaces to its Driver Services FRS. These are vetted and handled on an individual request basis. The existing Driver Services FRS has been utilized to identify suspects. No laws or regulations limit the current practice.
Missouri	No	No					The state of Missouri has a budget shortfall in the 2012. It does not appear that there will be any new technology deployments in State agencies in the general revenue pool including the Department of Revenue or Corrections.

State	1. Any Agency utilizing FRS	2. Intend to deploy FRS in 2011	3. Agencies utilizing FRS	4. Purpose of FRS	5. Compliance with REAL ID	6. Refuse to comply with Real ID	7. Relevant and/or interesting information relating to FRS
Nebraska	Yes		DL photos are maintained exclusively by the Nebraska Department of Motor Vehicles. Access of these photos is restricted to law enforcement and is available through the Nebraska Criminal Justice Information System, NCJIS.	Reduce issuance of multiple ID cards for the same person.	Unknown		There are strict dissemination restrictions on releasing DL photos in Nebraska per state statute. The Nebraska Department of Motor Vehicles safeguards the data and provides it for law enforcement purposes only. There are connectivity factors that perhaps could be explored. For addition information contact the Nebraska DMV.
Nevada	Yes		Used by the Department of Motor Vehicles	Reduce issuance of multiple ID cards for the same person.	Unknown		Nevada is in the process of implementing Real ID. The current status is unknown; the Department of Motor Vehicles is a separate Department from Public Safety. It appears that the DMV has had success using facial recognition technology.
New Hampshire	No	No					State regulations currently in place will substantially limit any ability to pursue this kind of technology. It does not appear that any consideration is being given to relax these restrictions. If anything, there will be additional limitations put in place to protect an individual's right to privacy.
New Jersey	Yes		Used by the NJ State Police Regional Operations Intelligence Center, R.O.I.C.	Law enforcement purpose can call the R.O. I C. for FRS. Unknown what DMV is using	Unknown		Currently funds have been frozen and future direction is unknown.
New Mexico	Yes		Used by the Motor Vehicle Department (MVD)	MVD for security and DL issuance reasons.	No, decision made by Executive Government	Yes	
New York	Yes		Used by the NYS Department of Motor Vehicles	Contact DMV	Yes		
North Carolina	Yes		Used by the Department of Motor Vehicles	Reduce fraud	Unknown		None
Ohio	Yes		Used by the Ohio Attorney General's Office Bureau of Criminal Identification and Investigation.	Ohio BCI&I (our Central Repository) is just starting a project to utilize FRS to assist law enforcement with positive identification through comparing mug shots and drivers license images and returning the images along with inquiries into the state computerized criminal histories.	Unknown		The implementation of the FRS project, as of now, is still a future deployment. OBCI&I would be the best contact for additional information.
Oklahoma	No	Unknown					Unknown at this time.
Oregon	Yes		Used by the Oregon Department of Motor Vehicles	DMV verification and fraud reduction	No	No	

State	1. Any Agency utilizing FRS	2. Intend to deploy FRS in 2011	3. Agencies utilizing FRS	4. Purpose of FRS	5. Compliance with REAL ID	6. Refuse to comply with Real ID	7. Relevant and/or interesting information relating to FRS
Rhode Island	Yes		Used by the RI Department of Motor Vehicles. The RI State Police fusion center leverages that DMV system to help police officers in local agencies with cases. RI Corrections may also uses facial recognition. In addition the Corrections Division recently began the use of iris scan technology to identify inmates.	DMV uses for investigation multiple licenses and fraud. Fusion Center uses for assisting with investigations	Unknown		The State's DMV is currently rebuilding their IT systems. The State Police, have obtained a grant to deliver license images to local and state law enforcement, in state, through our RILETS network. We have two years to spend the grant funding. We will begin the project as soon as the DMV system is complete. DMV system should be on line sometime during the summer of 2011.
Texas	Yes		Used by the Texas Department of Public Safety	It is part of the Driver License issuance process for numerous reasons including prevention of fraudulent applications.	Unknown		While FRS is used in state, it is not something that can be shared with other entities at this time due to privacy concerns.
Virginia	No	No					
Washington	No	Unknown					
West Virginia	No	No					The WV DMV is presently implementing a new drivers system at which time driver license photos will be available to law enforcement through our State switch. FRS technology may be reviewed after that time
Wisconsin	Yes		Possibly used by the Wisconsin Department of Motor Vehicles	Possibly to prevent duplicate credentials	Unknown		State statute 343.237 & 165.8287 limit use of driver photos including "The photograph shall not be used as part of a photo lineup or photo array."
Wyoming	No	No					To date limitations have been both budgetary and technological to leverage these capabilities.

B

Appendix B: Stop and Identify Laws by State

STATE	CITATION	INFORMATION THAT MUST BE DISCLOSED.
Alabama	Ala. Code §15-5-30 (West 2003)	Name, address, and explanation of actions
Arizona	Ari. Rev. Stat. Tit. 13, §2412 (2005)	Name only
Arkansas	Ark. Code Ann. §5-71-213(a)(1) (2004)	Police officer may request the person to identify himself and explain his presence and conduct (Loitering Statute)
Colorado	Colo. Rev. Stat. §16-3-103(1) (2003)	Name, address, and explanation of actions
Delaware	Del. Code Ann., Tit. 11, §§1902(a) , 1321(6) (2003)	Name, address, business abroad, and destination
Florida	Fla. Stat. §856.021(2) (2003)	Police officer may request the person to identify himself and explain his presence and conduct (Loitering Statute)
Georgia	Ga. Code Ann. §16-11-36(b) (2003)	Police officer may request the person to identify himself and explain his presence and conduct (Loitering Statute)
Illinois	Ill. Comp. Stat., ch. 725, §5/107-14 (2004)	Name, address, and explanation of actions
Indiana	Ind. Code §34-28-5-3.5 (1998)	Name, address, date of birth OR driver's license, if in the person's possession
Kansas	Kan. Stat. Ann. §22-2402(1) (2203)	Name, address, and explanation of actions
Louisiana	La. Code Crim. Proc. Ann., Art. 215.1(A) (West 2004)	Name, address, and explanation of actions
Missouri	Mo. Rev. Stat. §84.710(2) (2003)	Name, address, business abroad, and destination
Montana	Mont. Code Ann. §46-5-401(2)(a) (2003)	Officer may request the person's name, present address, and an explanation of the person's actions
Nebraska	Neb. Rev. Stat. §29-829 (2003)	Name, address, and explanation of actions
Nevada	Nev. Rev. Stat. §171.123(1) (2003)	Name only
New Hampshire	N. H. Rev. Stat. Ann. §594:2, 644:6 (Lexis 2003)	Name, address, business abroad, and destination
New Mexico	N. M. Stat. Ann. §30-22-3 (2004)	Name only
New York	N. Y. Crim. Proc. Law (CPL) §140.50(1) (West 2004)	Name, address, and explanation of actions
North Dakota	N.D. Cent. Code §29-29-21 (2003)	Name, address, and explanation of actions
Ohio	Ohio Rev. Code §2921.29 (2006)	Name, address, and date of birth
Rhode Island	R. I. Gen. Laws §12-7-1 (2003)	Name, address, business abroad, and destination
Utah	Utah Code Ann. §77-7-15 (2003)	Name, address, and explanation of actions
Vermont	Vt. Stat. Ann., Tit. 24, §1983 (Supp.2003)	Identify himself or herself satisfactorily to the officer
Wisconsin	Wis. Stat. §968.24 (2003)	Name, address, and explanation of actions

C

Appendix C: Issues Document

Issue identification: Privacy issues concerning the application of facial recognition technologies to identify subjects in the field via Nlets Data Exchanges is available upon request to provide additional context and areas of privacy concern that may not have been directly addressed in the report.

D

Appendix D:
Cross reference table to DHS Privacy Impact Assessment[151]

DHS Privacy Impact Assessment Section		PIA Reference
Section 1.0 Authorities and Other Requirements		
1.1	What specific legal authorities and/or agreements permit and define the collection of information by the project in question?	Part 5(B)
1.2	What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?	None; not applicable.
1.3	Has a system security plan been completed for the information system(s) supporting the project?	Part 9(E)
1.4	Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?	No, not applicable.
1.5	If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.	Not applicable.
Section 2.0 Characterization of the Information		
2.1	Identify the information the project collects, uses, disseminates, or maintains.	Part 5(A)
2.2	What are the sources of the information and how is the information collected for the project?	Parts 1(A); 1(B); 4(C)(1)
2.3	Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.	No.
2.4	Discuss how accuracy of the data is ensured.	Part 8
2.5	Privacy Impact Analysis: Related to Characterization of the Information	Parts 2(B); 2(C); 2(D); 5(C)
Section 3.0 Uses of the Information		
3.1	Describe how and why the project uses the information.	Parts 5(B); 6(B); 6(C)
3.2	Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.	No.
3.3	Are there other components with assigned roles and responsibilities within the system?	Part 1(A)
3.4	Privacy Impact Analysis: Related to the Uses of Information	Parts 2(E); 9(D)
Section 4.0 Notice		
4.1	How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.	Part 5(D)
4.2	What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?	Part 5(D)

[151] U.S. Dept. of Homeland Sec., Privacy Office, *Privacy Impact Assessment Template* (Version 05/11/2010).

DHS Privacy Impact Assessment Section		PIA Reference
4.3	Privacy Impact Analysis: Related to Notice	Part 5(D)
Section 5.0 Data Retention by the Project		
5.1	Explain how long and for what reason the information is retained.	Part 7
5.2	Privacy Impact Analysis: Related to Retention	Parts 7; 8(B)
Section 6.0 Information Sharing		
6.1	Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.	No.
6.2	Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.	Not applicable.
6.3	Does the project place limitations on re-dissemination?	Parts 6(B); 6(C)
6.4	Describe how the project maintains a record of any disclosures outside of the Department.	Parts 6(C); 7(D); 9(B)
6.5	Privacy Impact Analysis: Related to Information Sharing	Parts 2(E); 6(C); 9(A); 9(B); 9(C)
Section 7.0 Redress		
7.1	What are the procedures that allow individuals to access their information?	Part 8(B)
7.2	What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Part 8(B)
7.3	How does the project notify individuals about the procedures for correcting their information?	Part 5(D)
7.4	Privacy Impact Analysis: Related to Redress	Part 8(B)
Section 8.0 Auditing and Accountability		
8.1	How does the project ensure that the information is used in accordance with stated practices in this PIA?	Part 9
8.2	Describe what privacy training is provided to users either generally or specifically relevant to the project.	Part 9(D)
8.3	What procedures are in place to determine which users may access the information and how does the project determine who has access?	Parts 1(B); 5(B)
8.4	How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?	Not applicable.

E

Appendix E:
Cross reference table to DOJ Privacy Impact Assessment[152]

DOJ Privacy Impact Assessment Section		PIA Reference
Section 1: Description of the Information System		
(a)	the purpose that the records and/or system are designed to serve;	Part 5(C)
(b)	the way the system operates to achieve the purpose(s);	Part 1(B)
(c)	the type of information collected, maintained, used, or disseminated by the system;	Part 5(A)
(d)	who has access to information in the system;	Part 1(A)
(e)	how information in the system is retrieved by the user;	Parts 1; 6
(f)	how information is transmitted to and from the system;	Part 1(A)
(g)	any interconnections with other systems.	Part 1(A)
Section 2: Information in the System		
2.1	Indicate below what information is collected, maintained, or disseminated.	Part 5(A)
2.2	Indicate sources of the information in the system.	Parts 5(A); 5(B); 4(C)(1)
2.3	Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy.	Parts 3(B); 3(C); 3(D)
Section 3: Purpose and Use of the System		
3.1	Indicate why the information in the system is being collected, maintained, or disseminated.	Parts 5(C); 6(B); 6(C)
3.2	Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.	Parts 1(B); 6(B)
3.3	Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system.	Part 5(B)
3.4	Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period.	Part 7

[152] U.S. Dept. of Justice, Office of Privacy and Civil Liberties, *Privacy Impact Assessment Template* (August 2010).

DOJ Privacy Impact Assessment Section		PIA Reference
3.5	Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately.	Parts 3(B); 3(E); Part 7; Part 8(B)
Section 4: Information Sharing		
4.1	Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.	Parts 6(B); 6(C)
4.2	Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.	Parts 6(C); 7(C); 7(D); 9(A); 9(B); 9(C)
Section 5: Notice, Consent, and Redress		
5.1	Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system.	Part 5(D)
5.2	Indicate whether and how individuals have the opportunity to decline to provide information.	Parts 5(D); 5(B); 4(C)(1)
5.3	Indicate whether and how individuals have the opportunity to consent to particular uses of the information.	Part 5(B)
5.4	Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.	Part 5(D)
Section 6: Information Security		
6.1	Indicate all that apply.	Part 9(E)
6.2	Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.	Part 9(E)
Section 7: Privacy Act		
7.1	Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a.	No.
7.2	Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.	Part 1(A)