



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 31, 2012

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Jerome Pender, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, before the Subcommittee on Privacy, Technology and the Law on July 18, 2012, at a hearing entitled "What Facial Recognition Technology Means for Privacy and Civil Liberties." We hope that this information is of assistance to the Committee.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Judith C. Appelbaum
Acting Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Member

**Questions for the Record
Jerome Pender
Deputy Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation**

**Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate**

**“What Facial Recognition Technology Means for Privacy and Civil Liberties”
July 18, 2012**

Question Posed by Senator Franken

In 2009, the FBI used facial recognition technology to compare the photos of fugitives to the driver’s license photos in the North Carolina DMV. I’m told that the FBI is looking to expand this program. What plans, if any, does the FBI have to expand its DMV pilot, and how will it protect against innocent citizens getting falsely accused as a result of false positives?

Response:

“Project Facemask” was initiated in 2007 as a collaborative effort by the FBI and the North Carolina (NC) Department of Motor Vehicles (DMV) to use the NC DMV’s facial recognition program as a means of locating fugitives and missing persons. This pilot received national attention in 2009 when the NC driver’s license photograph of “Jose Luis Solis” was compared with a 1991 California booking photograph of double-homicide suspect Rodolfo Corrales. “Solis” was later confirmed to be Corrales, who was arrested in his NC home and extradited to California for prosecution. The project also resulted in the apprehension of six state fugitives and the resolution of one missing person case.

Upon the successful conclusion of the pilot in 2010, the capabilities were evaluated to assess the operational value of creating an FBI facial searching service. Based on this evaluation, the FBI created a Facial Analysis Comparison and Evaluation (FACE) Services Unit. The FACE Services Unit has begun establishing Memoranda of Understanding (MOUs) with the DMVs of states whose laws allow them to share DMV information for law enforcement purposes, as permitted by Federal law regarding the use of state motor vehicle records (18 U.S.C. §§ 2721-25). This process is being carried out in coordination with the Office of the General Counsel and the FBI’s Records Management Division to ensure compliance with laws, regulations, and policies governing this kind of information.

The FACE team will compare the facial images of subjects of active FBI investigations with images housed in select FBI databases and other databases to which the FBI has access for law enforcement purposes. In addition, for states with which we have established MOUs, FBI fugitives’ and subjects’ identities will also be queried in the DMV records, with the results

returned to the FACE team for comparison analysis.¹ The FACE team, consisting of personnel who have been specially trained in facial recognition comparisons, will identify any likely matches to the subject of the FBI investigation.

While the procedures will vary somewhat by state, typically the DMV will receive an inquiry from the FBI and will conduct an automated search of its image repository (in NC, for example, this search is conducted using a facial recognition algorithm). The DMV will provide image galleries to FACE Services Unit specialists, who will conduct manual comparisons in order to exclude unassociated persons and to identify any likely candidates. A blind verification ("double check") will then be conducted as part of the internal quality review process. If this confirms the original identification, the results of the manual comparison will be provided to the Special Agent working the open case with the caution that the information is to be used for lead purposes only. The case Agent will be responsible for further investigation to determine whether any possible matches are relevant to the investigation.

Communications with DMVs regarding facial recognition services will be conducted through a secure e-mail portal, and incoming and outgoing case work will be tracked and stored in an internal work log. This information will be retained for audit purposes. Access to the FACE Services Unit work log will be limited to that unit and to other authorized FBI personnel who need access to the log for audit or legal purposes. The FACE Services team is well aware of the need to conduct its activities in a manner that protects civil liberties. Therefore, in order to protect the civil liberties of innocent individuals, procedures have been developed to ensure that the FACE team appropriately disposes of any personally identifiable information (both hard copy and electronic) of individuals determined not to be candidate matches.

¹ Among other protections, all MOUs require that participating states protect privacy by: ensuring that the photos related to an FBI inquiry are not transmitted in internal or external state systems except through secure Law Enforcement Online transmissions; mandating the immediate, permanent, and appropriate destruction of these photos and related records once the inquiry is answered; and ensuring that states comply with their privacy laws and immediately report any unauthorized information dissemination or loss.