REPORT OF THE
VIRGINIA STATE CRIME COMMISSION

HB 454
Facial Recognition Technology by Virginia Law Enforcement Agencies

A BILL REFERRAL STUDY TO THE
SENATE COURTS COMMITTEE AND
THE GENERAL ASSEMBLY OF VIRGINIA

COMMONWEALTH OF VIRGINIA
RICHMOND
DECEMBER 2002

I. Authority

The *Code of Virginia*, § 30-156, authorizes the Virginia State Crime Commission to study, report and make recommendations on all areas of public safety and protection. Additionally, the Commission is to study matters "including apprehension, trial and punishment of criminal offenders." Section 30-158(3) provides the Commission the power to "conduct studies and gather information and data in order to accomplish its purposes as set forth in § 30-156. . .and formulate its recommendations to the Governor and the General Assembly."

Using the statutory authority granted to the Crime Commission, the staff conducted a study to determine whether legislation should be adopted to regulate the use of facial recognition technology by law enforcement in the Commonwealth.

II. Executive Summary

During the 2002 Session of the Virginia General Assembly, Delegate H. Morgan Griffith introduced House Bill 454 (HB 454),[1] which would have added a chapter to the *Code of Virginia* governing the applications for, and limiting the use of, facial recognition technology by Virginia law enforcement agencies. This bill was communicated to the Senate, where it was referred to the Senate Courts of Justice Committee. The Committee continued the bill until 2003 and referred it by letter to the Virginia State Crime Commission for further study. As a result of this study effort, the following recommendation was made concerning HB 454.

Recommendation

The Crime Commission recommends an alternative approach for governing the use of facial recognition technology by Virginia law enforcement agencies. Rather than create an application process wherein a Circuit Court must be petitioned and then issues an Order of finite duration whenever a law enforcement agency wishes to make use of such technology, the *Code of Virginia* can be modified to limit the types of information which law enforcement agencies may gather through this technology. Additional limitations can be placed on law enforcement agencies concerning the use and distribution of such information, and provisions can be made for the expungement of data which is obsolete, unreliable, or misleading. To ensure compliance with these requirements, the Department of Criminal Justice Services can be assigned the task of monitoring and periodically auditing the data gathered by law enforcement through facial recognition technology.

[1] After House Bill 454 (2002) was introduced, a substantially similar version of the same bill was substituted in the House. This substitute bill, with its one amendment, hereinafter shall be referred to as HB 454. *See Attachment 1.*

III. Methodology

The Virginia State Crime Commission utilized three research methodologies to examine HB 454. First, the proposed legislation was examined and compared with similar existing provisions in the *Code of Virginia*. Next, a legal analysis of the issues involved with facial recognition technology was conducted, examining in particular any possible constitutional limitations or mandates. Finally, the *Code of Federal Regulations* was consulted for insight into how possible problems with this technology might be addressed.

IV. Background

Facial recognition technology is a biometric technology that records the spatial geometry of facial features. Typically, a photograph or image of an individual's face is converted into a number of measurements (such as the distance between the eyes, the distance between the nose and the corners of the eyes, the length and width of the mouth, etc.), which in turn is used to create a mathematical "faceprint," or template. Once a template has been created, a computer can quickly compare it with previously entered templates to see if there is a match, in a process similar to that used for comparing or identifying fingerprints.[2]

It should be noted that while this technology is commonly associated with public video cameras,[3] the technology proper does not consist of the camera, but rather the computer program that processes the images from that camera. A video camera that is monitored solely by a human operator is not facial recognition technology.[4]

When a law enforcement agency uses such technology, a question may arise as to whether the Constitution of the United States places any limits on the scope of such use. Generally, law enforcement is prohibited, under the Fourth Amendment, from conducting "unreasonable searches and seizures." However, as long as the initial gathering of a person's image is taken in a public place, the "search" involved in such activity is almost certainly permissible under the Constitution.

The United States Supreme Court has stated, "no interest legitimately protected by the Fourth Amendment is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into the security a man relies upon when he places himself or his property within a constitutionally protected area."[5] As a result,

[2] *See, generally*, Woodward, John D., Jr., *Biometrics: Facing Up to Terrorism*, Santa Monica, CA: RAND, IP-218 (2001); Woodward, John D., Jr., *Super Bowl Surveillance: Facing Up to Biometrics*, Santa Monica, CA: RAND, IP-209 (2001).

[3] *See, supra* Woodward, John D., Jr., *Super Bowl Surveillance: Facing Up to Biometrics*.

[4] HB 454 recognizes this distinction. It specifically defines "facial recognition technology" as "**any technology or software system employed for the purpose of matching a facial image** captured by cameras placed in any public place…with an image stored in a database." (Emphasis supplied).

[5] United States v. Miller, 425 U.S. 435, 440 (1976) (*additional citations omitted).*

"what a person knowingly exposes to the public…is not a subject of Fourth Amendment protection."[6]

For instance, in United States v. Knotts, the Supreme Court wrote, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[7] The Court reasoned that "[w]hen [an individual] travel[s] over the public streets he voluntarily convey[s] to anyone who want[s] to look the fact that he [is] traveling over particular roads in a particular direction…."[8] In dicta even more germane to the issue of facial recognition technology, the Supreme Court stated, "No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world."[9]

Therefore, it would appear that as long as facial recognition technology is used only in connection with images captured by video cameras located and focused on public areas, no constitutional problems arise.

V. Analysis of House Bill 454

House Bill 454 would mandate a procedure whereby every time a law enforcement agency wished to make use of facial recognition technology, they would have to seek prior court approval. "Facial recognition technology" is defined in the bill as "any technology or software system employed for the purpose of matching a facial image captured by cameras placed in any public place." Therefore, the bill would have no impact on the ability of police departments to place video cameras throughout a public area. The only limitation would be in employing a computer system to analyze the images captured by video cameras.[10] The bill does make two exceptions: areas in state or local correctional facilities are exempted, as are public-use airports, harbors and seaports.

Under HB 454, if a law enforcement agency wished to make use of facial recognition technology, they could only do so for limited purposes: to gather evidence of the commission of a felony or Class 1 misdemeanor; search for persons with outstanding felony warrants; search for persons who are affiliated with a terrorist organization; or search for missing persons. In seeking court approval, law enforcement could not petition the Circuit Court directly, but would have to work through the auspices of either the Attorney General's Office, or through a Commonwealth's Attorney.

The application for the Circuit Court Order would have to be made in writing, and assert under oath: the identity of the applicant; the nature of the information sought, the

[6] Katz v. United States, 389 U.S. 347, 351 (1967).
[7] United States v. Knotts, 368 U.S. 276, 281-82 (1983).
[8] *Id.*
[9] United States v. Dionisio, 410 U.S. 1, 14 (1973).
[10] The bill would also have no impact on the placing of video cameras in private areas OR the use of such technology with such cameras. Unlike images captured in public, this activity by law enforcement would, of course, be governed by basic Fourth Amendment limitations.

location of the facilities where the facial recognition technology is to be used, the identity of the person or class of persons sought, and a description of the database to be used in the matching process; the period of time in which the technology would be used; a full and complete statement of facts concerning all previous applications made to use such technology involving any of the same persons, facilities, or places; and, in reapplications, the reason for the failure to obtain expected results.

The bill would create stringent time limitations on the use of facial recognition technology by law enforcement. An initial application could not be for any period longer than ninety days. After the initial ninety days, the agency could seek an extension of the Order for an additional sixty days.

All Orders granted by a Circuit Court would have to detail much of the same information included in the application, and specify that the facial recognition technology be used only for those purposes, and only by the authorized agency. In addition, the Order would require that any facial images captured that were not relevant to the investigation would have to be disposed of in at most ten days. If the court wished, it could require periodic reports detailing the progress of the investigation and the need for continued use of the facial recognition technology.

Finally, any violation of any of these provisions by a law enforcement agent could be punished as contempt of court.

The extensive requirements under this process, both for seeking an authorizing Circuit Court Order and for what a circuit court can allow under the law, strongly parallel the procedures involved in seeking a wiretap warrant.[11] Although only the Attorney General's Office can apply for a wiretap warrant,[12] and this bill would allow Commonwealth's Attorneys as well as the Attorney General's Office to apply for a facial recognition technology Order, the detailed requirements in both applications mirror each other.[13] (Also, wiretap Orders run for only thirty days, not ninety, and can be extended for an additional thirty days, rather than sixty days).[14] Because the Fourth Amendment usually requires some type of judicial authorization before law enforcement engages in the interception of oral communications,[15] the extensive provisions of Chapter 6 of Title 19.2 of the *Code of Virginia* are necessary. However, as noted above, the Fourth Amendment does not come into play when images captured by video cameras are gathered from public locations. Therefore, the use of facial recognition technology by the police would not be prohibited, even if HB 454 were not passed into law.

[11] *See*, *Va. Code* §§ 19.2-61 through 19.2-70.3. This is indirectly recognized by the fact that the current wiretapping provisions are found in Chapter 6 of Title 19.2, while the provisions of HB 454 would be placed in a new Chapter 6.1.

[12] *Va. Code* § 19.2-66.

[13] *See*, *Va. Code* § 19.2-68.

[14] *Va. Code* § 19.2-68(D).

[15] Katz v. United States, 389 U.S. 347 (1967).

VI. Conclusion

In essence, the provisions of HB 454 severely limit law enforcement's use of facial recognition technology, and condition any use upon judicial approval. Even though the Fourth Amendment does not require any judicial approval whatsoever for this technology to be implemented, a state is always free to restrict the activities of law enforcement. Whether it chooses to do so in certain categories of activity is a matter of public policy.[16]

It must be recognized that when it comes to the use of facial recognition technology, various privacy concerns, in a general rather than legal sense, arise.[17] In fact, the United States Supreme Court has recognized, in dicta, that it is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[18] Certainly, if law enforcement were to use facial recognition technology for purposes of tracking or identifying a person's religious or political affiliations, it raises the specter of impermissible government intrusion into the private lives of ordinary citizens. However, facial recognition technology also offers law enforcement a useful technological tool which validly could be used to help monitor public areas. "[W]hile civil libertarians might decry the use of this technology as an invasion of privacy, the key lies in balancing the need for security with the need to protect civil liberties."[19]

One way to obtain such a balance would be for the legislature to restrict, not the overall use of such technology, but any improper uses that law enforcement might attempt. Currently, the *Code of Federal Regulations* promulgates a series of regulations concerning the types of data that can be stored in any criminal intelligence system that receives funding under the Omnibus Crime Control and Safe Streets Act of 1968.[20] Such data includes all forms of criminal intelligence information, and thus would pertain to photographs and facial recognition templates. Under these regulations, a law enforcement agency can only collect and maintain criminal intelligence information on an individual if "there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity."[21] Agencies are strictly prohibited from collecting or maintaining information about the "political, religious or social views, associations, or activities" of any individual, corporation, association or group, unless such information directly relates to criminal

[16] For instance, the City of Virginia Beach has passed a City Ordinance regulating and restricting the use of facial recognition technology by the Virginia Beach Police Department. *See Attachment 2*.

[17] For a brief discussion of such concerns, *see* Woodward, John D., Jr., *Super Bowl Surveillance: Facing Up to Biometrics*, sections titled, "Privacy Concerns of Current Uses," and "Potential Privacy Concerns as the Technology Advances," Santa Monica, CA: RAND, IP-209 (2001).

[18] Whalen v. Roe, 429 U.S. 589, 605 (1977).

[19] Woodward, John D., Jr., *Biometrics: Facing Up to Terrorism*, p. 15, Santa Monica, CA: RAND, IP-218 (2001).

[20] 28 C.F.R. §§ 23.1 through 23.40. Many of Virginia's criminal intelligence systems come under the requirements of these sections.

[21] 28 C.F.R. § 23.20(a).

conduct or activity.[22] Additional regulations strictly control the dissemination of criminal intelligence information (on a "need to know and a right to know basis"), and require careful records to be kept of any dissemination.[23] Information must be safeguarded to prevent unauthorized access,[24] and all information must be periodically reviewed, so that any obsolete, misleading or otherwise unreliable data can be deleted or destroyed.[25] Periodic audits of information systems are required to ensure compliance with these regulations.[26]

The Virginia legislature could adopt many of these requirements and make them into law. The Virginia Department of Criminal Justice Services (DCJS) could be entrusted with instructing law enforcement agencies on the proper uses of facial recognition technology, as well as what is impermissible. Additionally, DCJS could monitor and audit all information gathered in connection with facial recognition technology. In this way, law enforcement could make use of a potentially helpful surveillance and identification tool, without the cumbersome restrictions inherent in continually seeking court approval every few months. At the same time, safeguards would be placed into law, preventing law enforcement from misusing this technology in ways that the public might find troublesome.

[22] 28 C.F.R. § 23.20(b).
[23] 28 C.F.R. § 23.20(e) and (g).
[24] 28 C.F.R. § 23.20(g).
[25] 28 C.F.R. § 23.23.20(h).
[26] 28 C.F.R. § 23.40.

VII. Acknowledgments

The Virginia State Crime Commission extends its appreciation to the following agencies and individuals for their assistance and cooperation on this study.

RAND Corporation
Mr. John D. Woodward, Jr., Senior Policy Analyst

Virginia Beach Police Department
Chief A.M. Jacocks, Jr., Virginia Beach Police Department

Virginia State Police