DOCUMENTED BRIEFING

RAND

Biometrics

A Look at Facial Recognition

John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas

Prepared for the
Virginia State Crime Commission

RAND Public Safety and Justice

The research described in this report was conducted by RAND Public Safety and Justice for the Virginia State Crime Commission.

ISBN: 0-8330-3302-6

The RAND documented briefing series is a mechanism for timely, easy-to-read reporting of research that has been briefed to the client and possibly to other audiences. Although documented briefings have been formally reviewed, they are not expected to be comprehensive or definitive. In many cases, they represent interim work.

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND® is a registered trademark. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

© Copyright 2003 RAND

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2003 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Email: order@rand.org

PREFACE

During the 2002 General Assembly, Delegate H. Morgan Griffith sponsored legislation that would set legal parameters for public sector use of facial recognition technology in Virginia. The legislation, known as House Bill No. 454 (included as an Appendix), passed the House of Delegates by a vote of 74-25 earlier this year, and is pending in the Senate Courts of Justice Committee while the Virginia State Crime Commission examines it. The Virginia State Crime Commission, a standing legislative commission of the Virginia General Assembly, is statutorily mandated to make recommendations on all areas of public safety in the Commonwealth of Virginia.

Currently, Virginia Beach is the only municipality in Virginia planning to incorporate facial recognition technology into its public safety efforts. Late last year, the Virginia Beach City Council approved a measure authorizing the installation of a facial recognition system in the city's "Oceanfront" tourist area. The system has been tested and has recently been fully implemented.

Senator Kenneth W. Stolle, the Chairman of the Virginia State Crime Commission, established a Facial Recognition Technology Sub-Committee to examine the issue of facial recognition technology. Members of the Sub-Committee included: Senator Kenneth W. Stolle, Delegate H. Morgan Griffith, Delegate David B. Albo, Delegate Brian J. Moran, Superintendent W. Gerald Massengill of the Virginia State Police, Rich Savage of the Attorney General's Office, Chief A.M. Jacocks, Jr. of the Virginia Beach Police, and John D. Woodward, Jr. of RAND. In his capacity as a member, Mr. Woodward gave an informational presentation to the Sub-Committee on August 13, 2002 on which this documented briefing is based.

This briefing begins by defining biometrics and discussing examples of the technology. It then explains how biometrics may be used for authentication and surveillance purposes. Facial recognition is examined in depth, to include technical, operational, and testing considerations. This briefing concludes with a discussion of the legal status quo with respect to public sector use of facial recognition. While not making a specific policy recommendation with respect to House Bill No. 454, this briefing hopefully provides useful information for Sub-Committee members, the Virginia State Crime Commission, and other interested parties.

ACKNOWLEDGEMENTS

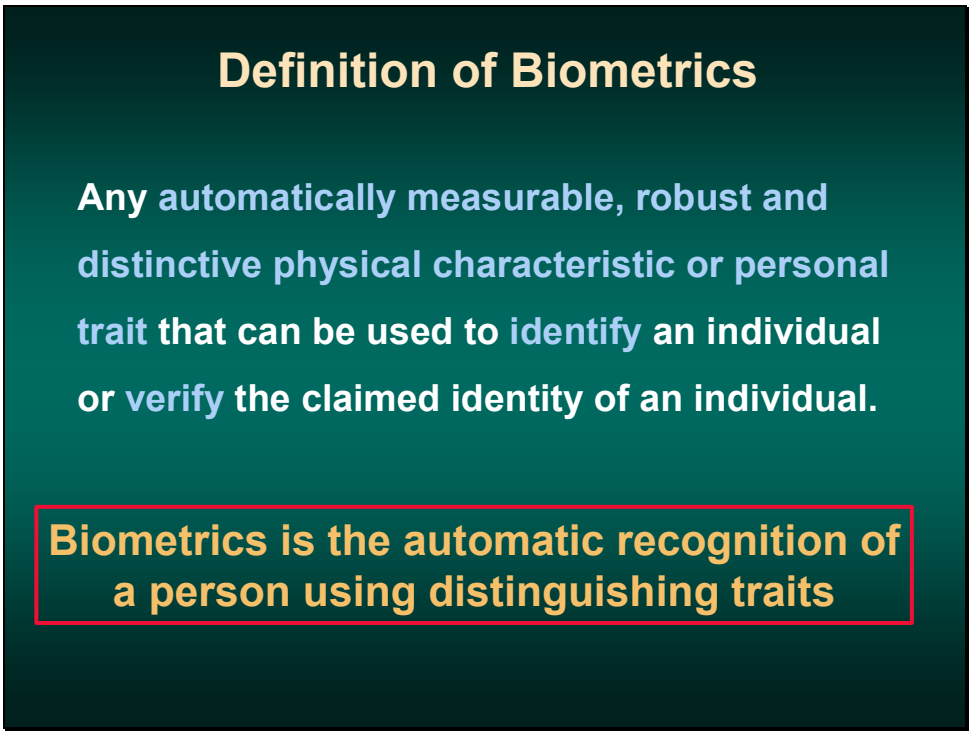
RAND Public Safety and Justice supported Mr. Woodward's work on behalf of the Virginia State Crime Commission. Christopher Horn and Aryn Thomas of RAND and Julius Gatune, a student at the RAND Graduate School, helped author this documented briefing. Dr. Jack Riley, the Director of RAND Public Safety and Justice, and Dr. Ken Horn of RAND's Arroyo Center provided helpful comments and assistance. Kimberly Hamilton and her staff at the Virginia State Crime Commission provided excellent logistical and operational support.

RAND is a nonprofit institution that helps improve policy and decision-making through research and analysis. RAND has a regional office in Arlington, Virginia.

CONTENTS

Preface i
Acknowledgements ii
Contents iii
Discussion of Biometrics 1
Discussion of Facial Recognition 7
Discussion of Legal Status Quo 17
Conclusions 20
Appendix 21
Selected Bibliography 25

DISCUSSION OF BIOMETRICS



A concise definition of biometrics is "the automatic recognition of a person using distinguishing traits." A more expansive definition of biometrics is "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual." This definition requires elaboration.

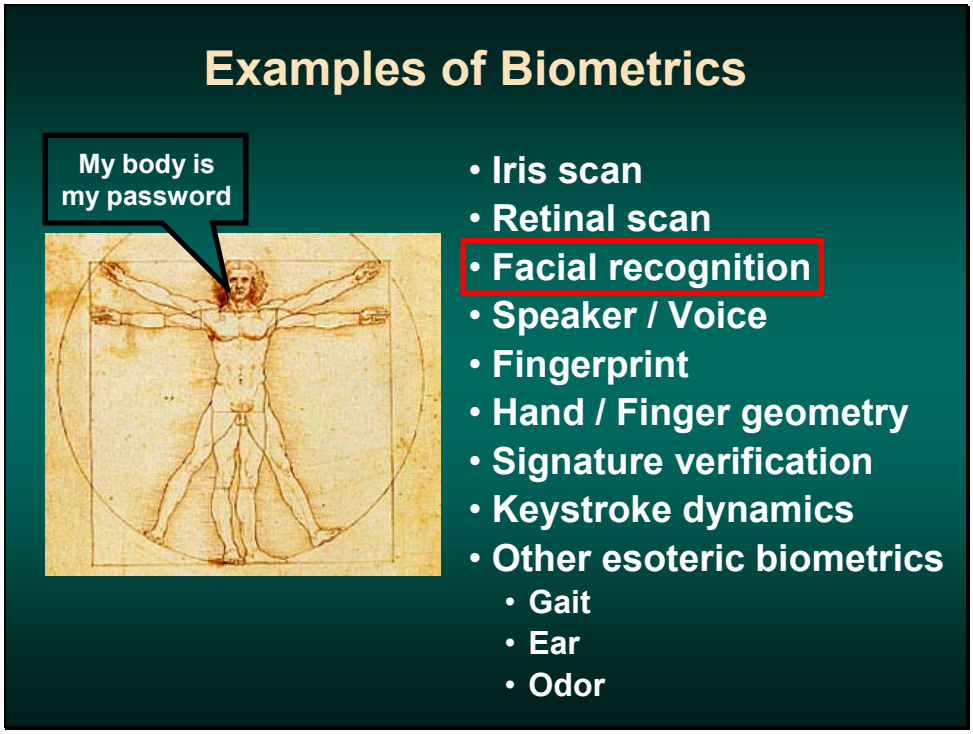
Measurable means that the characteristic or trait can be easily presented to a sensor, located by it, and converted into a quantifiable, digital format. This measurability allows for matching to occur in a matter of seconds and makes it an automated process.

The *robustness* of a biometric refers to the extent to which the characteristic or trait is subject to significant changes over time. These changes can occur as a result of age, injury, illness, occupational use, or chemical exposure. A highly robust biometric does not change significantly over time while a less robust biometric will change. For example, the iris, which changes very little over a person's lifetime, is more robust than one's voice.

Distinctiveness is a measure of the variations or differences in the biometric pattern among the general population. The higher the degree of distinctiveness, the more individual is the identifier. A low degree of distinctiveness indicates a biometric pattern found frequently in the general population. The iris and the retina have higher degrees of distinctiveness than hand or finger geometry.

Biometrics are used for human recognition which consists of *identification* and *verification*. The terms differ significantly. With *identification*, the biometric system asks and attempts to answer the question, "Who is X?" In an identification application, the biometric device reads a sample and compares that sample against every record or template in the database. This type of comparison is called a "one-to-many" search (1:N). Depending on how the system is designed, it can make a "best" match, or it can score possible matches, ranking them in order of likelihood. Identification applications are common when the goal is to identify criminals, terrorists, or other "wolves in sheep's clothing," particularly through surveillance.

Verification occurs when the biometric system asks and attempts to answer the question, "Is this X?" after the user claims to be X. In a verification application, the biometric system requires input from the user, at which time the user claims his identity via a password, token, or user name (or any combination of the three). This user input points the system to a template in the database. The system also requires a biometric sample from the user. It then compares the sample to or against the user-defined template. This is called a "one-to-one" search (1:1). The system will either find or fail to find a match between the two. Verification is commonly used for physical or computer access.



Biometric technologies may seem exotic, but their use is becoming increasingly common, and in 2001 *MIT Technology Review* named biometrics as one of the "top ten emerging technologies that will change the world." While this briefing focuses on facial recognition, there are many different types of biometrics as Leonardo DaVinci's *Vitruvian Man* makes clear. Examples include:

Iris Scan

Iris scanning measures the iris pattern in the colored part of the eye, although the iris color has nothing to do with the biometric. Iris patterns are formed randomly. As a result, the iris patterns in a person's left and right eyes are different, and so are the iris patterns of identical twins. Iris scanning can be used quickly for both identification and verification applications because the iris is highly distinctive and robust.

Retinal Scan

Retinal scans measure the blood vessel patterns in the back of the eye. The device involves a light source shined into the eye of a user who must be standing very still within inches of the device. Because users perceive the technology to be somewhat intrusive, retinal scanning has not gained popularity; currently retinal scanning devices are not commercially available.

Facial Recognition

Facial recognition records the spatial geometry of distinguishing features of the face. Different vendors use different methods of facial recognition, however, all focus on measures of key features of the face. Because a person's

face can be captured by a camera from some distance away, facial recognition has a clandestine or covert capability (*i.e.* the subject does not necessarily know he has been observed). For this reason, facial recognition has been used in projects to identify card counters or other undesirables in casinos, shoplifters in stores, criminals and terrorists in urban areas.

Speaker / Voice Recognition

Voice or speaker recognition uses vocal characteristics to identify individuals using a pass-phrase. A telephone or microphone can serve as a sensor, which makes it a relatively cheap and easily deployable technology. However, voice recognition can be affected by environmental factors such as background noise. This technology has been the focus of considerable efforts on the part of the telecommunications industry and the U.S. government's intelligence community, which continue to work on improving reliability.

Fingerprint

The fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies. The biometric device involves users placing their finger on a platen for the print to be electronically read. The minutiae are then extracted by the vendor's algorithm, which also makes a fingerprint pattern analysis. Fingerprint biometrics currently have three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) generally used for law enforcement purposes, fraud prevention in entitlement programs, and physical and computer access.

Hand/Finger Geometry

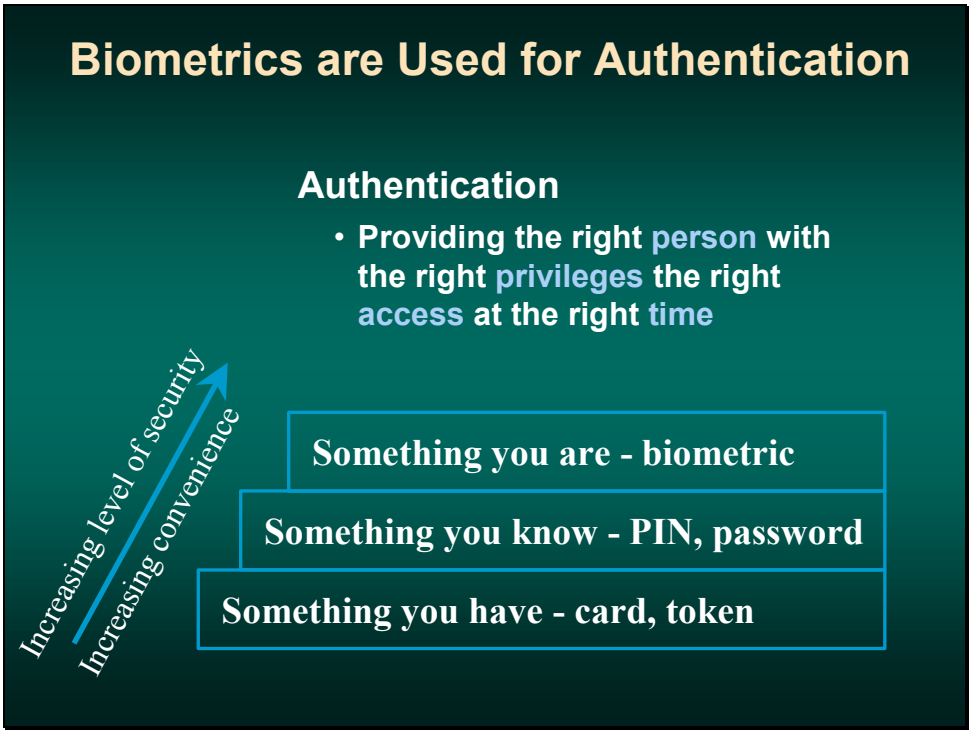
Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods takes actual prints of the palm or fingers. Spatial geometry is examined as the user puts his hand on the sensor's surface and uses guiding poles between the fingers to properly place the hand and initiate the reading. Finger geometry usually measures two or three fingers. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users. Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications.

Dynamic Signature Verification

We have long used a written signature as a means to acknowledge our identity. Dynamic signature verification is an automated method of measuring an individual's signature. This technology examines such dynamics as speed, direction, and pressure of writing; the time that the stylus is in and out of contact with the "paper," the total time taken to make the signature; and where the stylus is raised from and lowered onto the "paper."

Keystroke Dynamics

Keystroke dynamics is an automated method of examining an individual's keystrokes on a keyboard. This technology examines such dynamics as speed and pressure, the total time taken to type particular words, and the time elapsed between hitting certain keys. This technology's algorithms are still being developed to improve robustness and distinctiveness. One potentially useful application that may emerge is computer access, where this biometric could be used to verify the computer user's identity continuously.

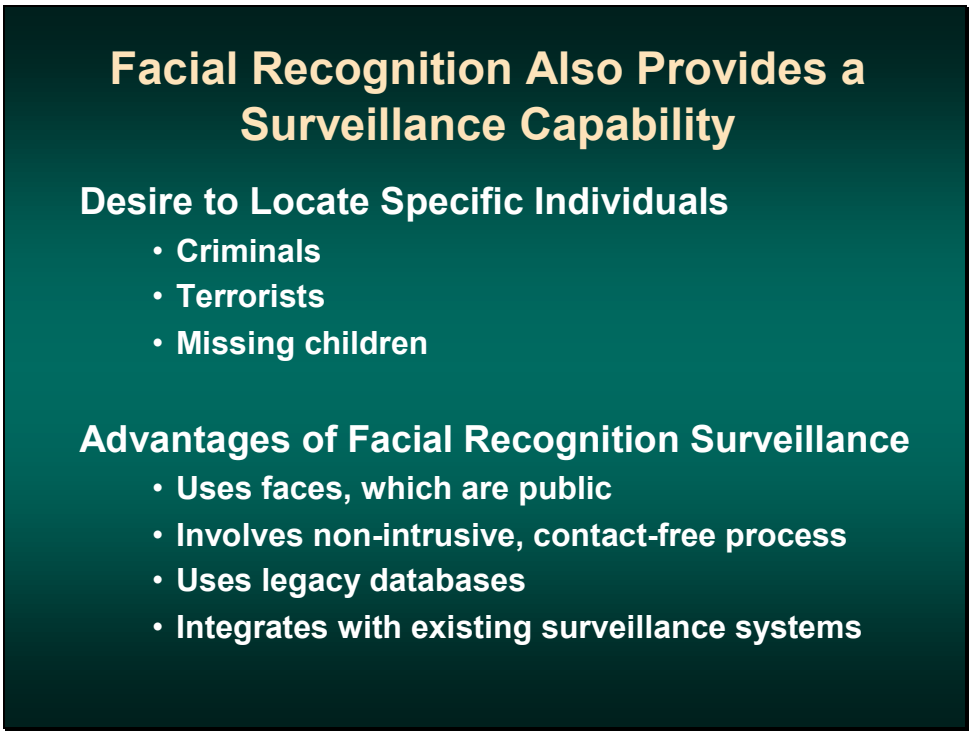


Authentication may be defined as "providing the right person with the right privileges the right access at the right time." In general, there are three approaches to authentication. In order of least secure and least convenient to most secure and most convenient, they are:

- Something you **have** - card, token, key.
- Something you **know**- PIN, password.
- Something you **are** - a biometric.

Any combination of these approaches further heightens security. Requiring all three for an application provides the highest form of security.

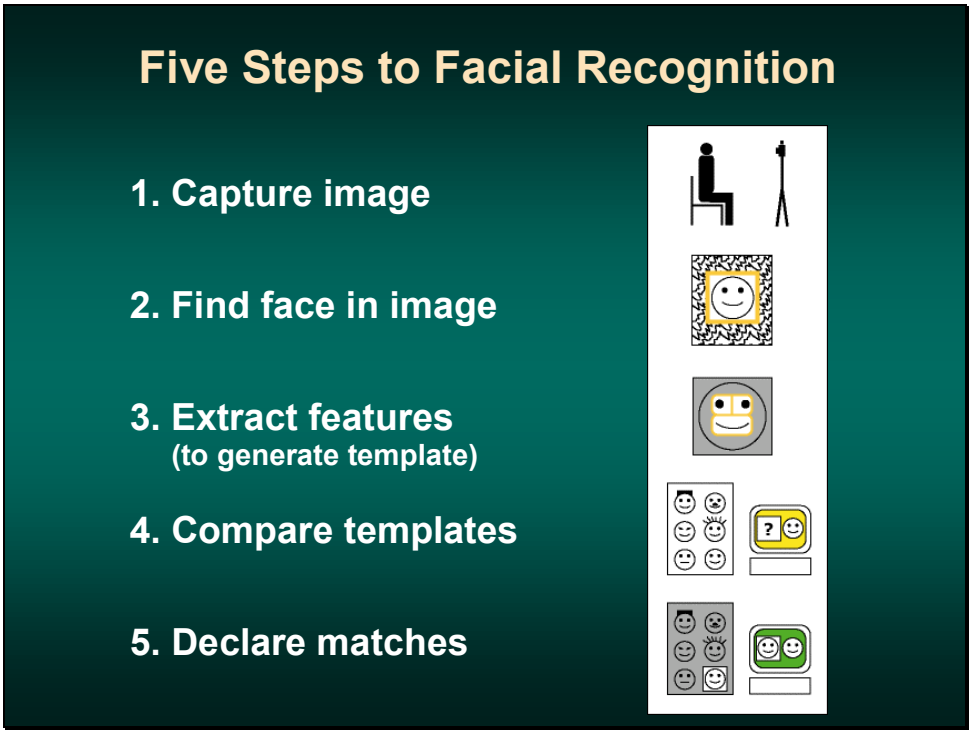
DISCUSSION OF FACIAL RECOGNITION



Although the concept of recognizing someone from facial features is intuitive, facial recognition, as a biometric, makes human recognition a more automated, computerized process. What sets apart facial recognition from other biometrics is that it can be used for surveillance purposes. For example, public safety authorities want to locate certain individuals such as wanted criminals, suspected terrorists, and missing children. Facial recognition may have the potential to help the authorities with this mission.

Facial recognition offers several advantages. The system captures faces of people in public areas, which minimizes legal concerns for reasons explained below. Moreover, since faces can be captured from some distance away, facial recognition can be done without any physical contact. This feature also gives facial recognition a clandestine or covert capability.

For any biometric system to operate, it must have records in its database against which it can search for matches. Facial recognition is able to leverage existing databases in many cases. For example, there are high quality mugshots of criminals readily available to law enforcement. Similarly, facial recognition is often able to leverage existing surveillance systems such as surveillance cameras or closed circuit television (CCTV).

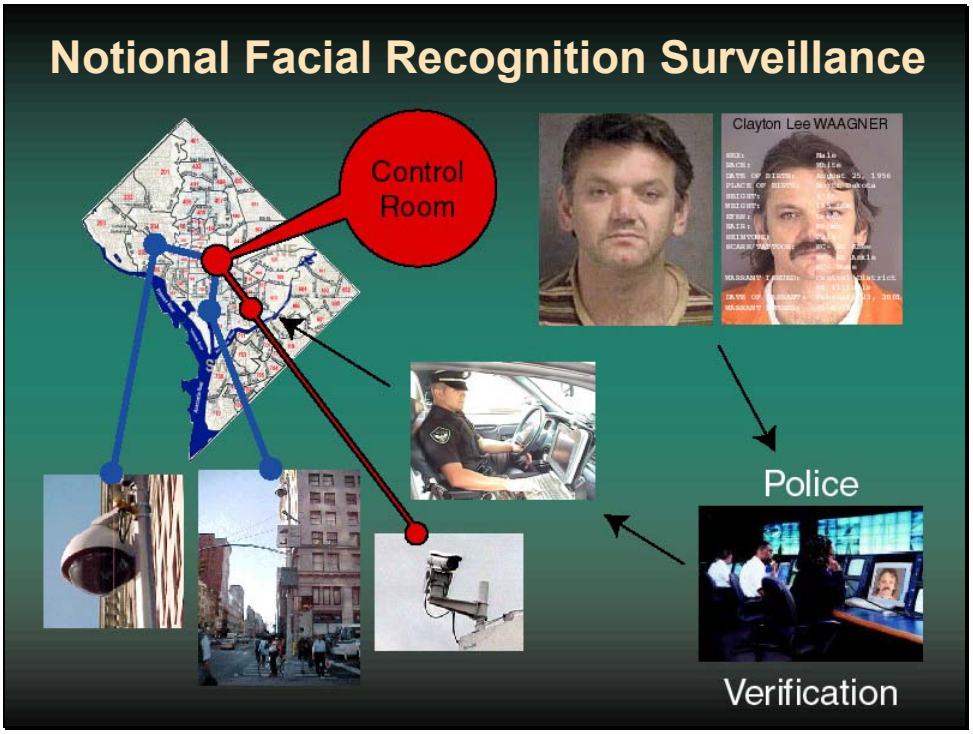


As a biometric, facial recognition is a form of computer vision that uses faces to attempt to identify a person or verify a person's claimed identity. Regardless of specific method used, facial recognition is accomplished in a five step process.

1. First, an image of the face is acquired. This acquisition can be accomplished by digitally scanning an existing photograph or by using an electro-optical camera to acquire a live picture of a subject. As video is a rapid sequence of individual still images, it can also be used as a source of facial images.
2. Second, software is employed to detect the location of any faces in the acquired image. This task is difficult, and often generalized patterns of what a face "looks like" (two eyes and a mouth set in an oval shape) are employed to pick out the faces.
3. Once the facial detection software has targeted a face, it can be analyzed. As noted in slide three, facial recognition analyzes the spatial geometry of distinguishing features of the face. Different vendors use different methods to extract the identifying features of a face. Thus, specific details on the methods are proprietary. The most popular method is called Principle Components Analysis (PCA), which is commonly referred to as the eigenface method. PCA has also been combined with neural networks and local feature analysis in efforts to enhance its performance. Template generation is the result of the feature extraction process. A template is a reduced set of data that represents the unique features of an enrollee's face. It is important to note that because the systems use spatial geometry of distinguishing facial

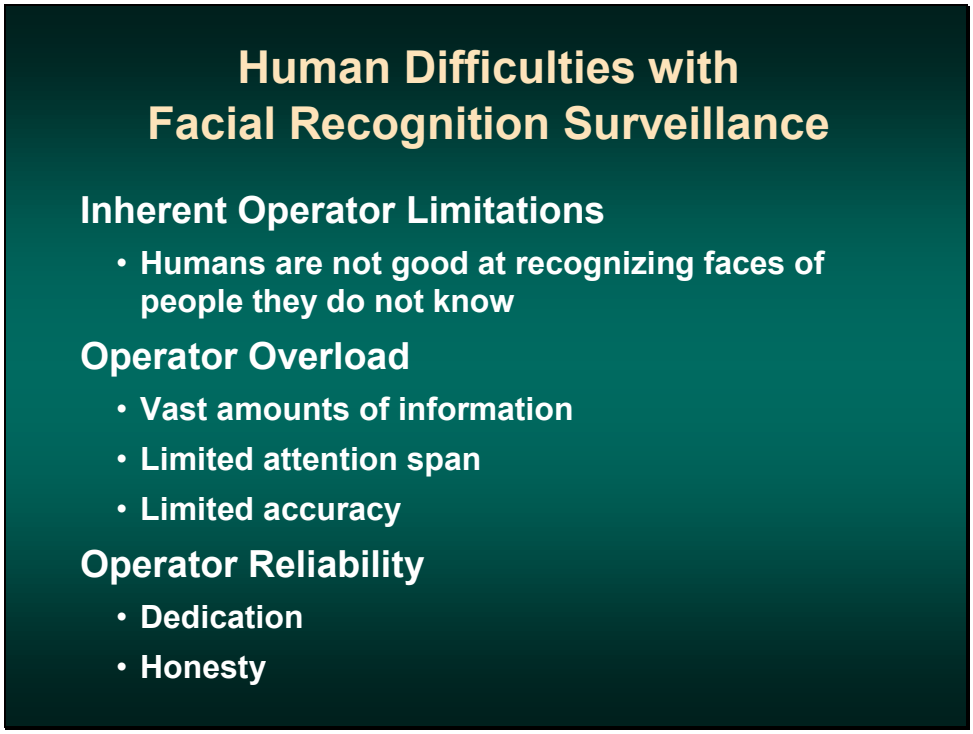
features, they do not use hairstyle, facial hair, or other similar factors.

4. The fourth step is to compare the template generated in step three with those in a database of known faces. In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity.
5. The final step is determining whether any scores produced in step four are high enough to declare a match. The rules governing the declaration of a match are often configurable by the end user, so that he or she can determine how the facial recognition system should behave based on security and operational considerations.



This graphic depicts a notional facial recognition surveillance system. Read clockwise from the lower left-hand corner, this system identifies and locates "targets" (*e.g.*, criminals, suspect terrorists, missing children) through a networked system of surveillance cameras (or CCTV).

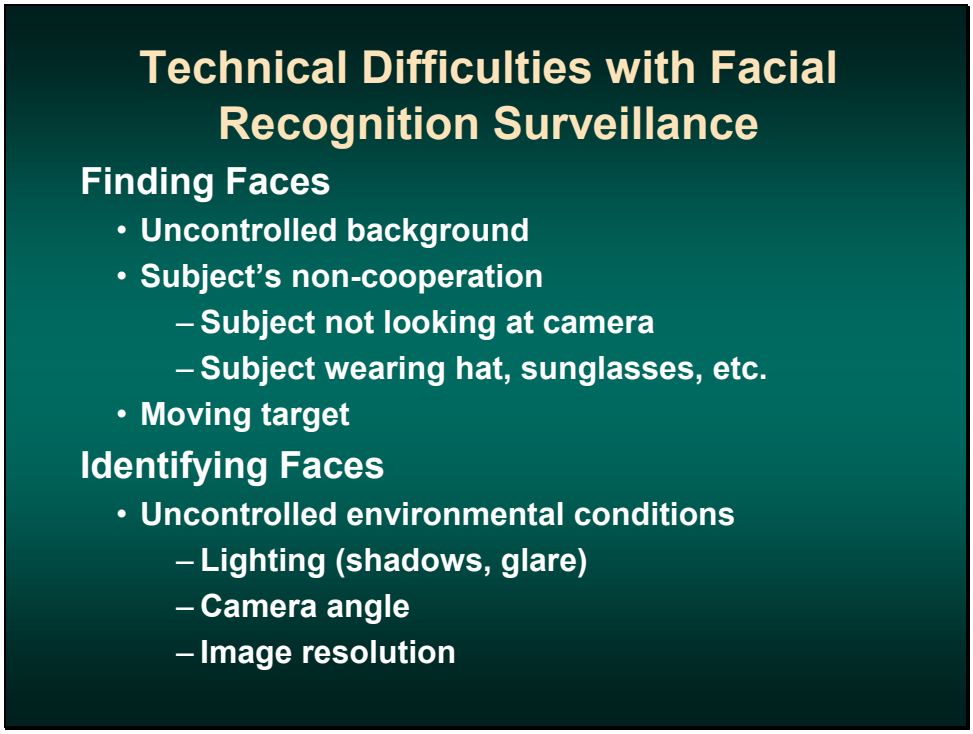
Video streams are sent over a network to a central control facility (*e.g.*, "Control Room"). At that central facility, computers find faces in the video, and then attempt to find a match in a database of target individuals. If a probable match is found, the system alerts an officer; it presents him with the image of the suspected match, as well as the image of the individual in the database. This verification step uses trained officers to ensure that false alarms generated by the system are caught and recorded. If the officer decides that the match is not a false alarm, he forwards the alert to officers on patrol, who are in the vicinity of where the original camera filmed the suspect.



People are generally very good at recognizing faces that they know. However, people experience difficulties when they perform facial recognition in a surveillance or watch post scenario. Several factors account for these difficulties: most notably, humans have a hard time recognizing unfamiliar faces. Combined with relatively short attention spans, it is difficult for humans to pick out unfamiliar faces.

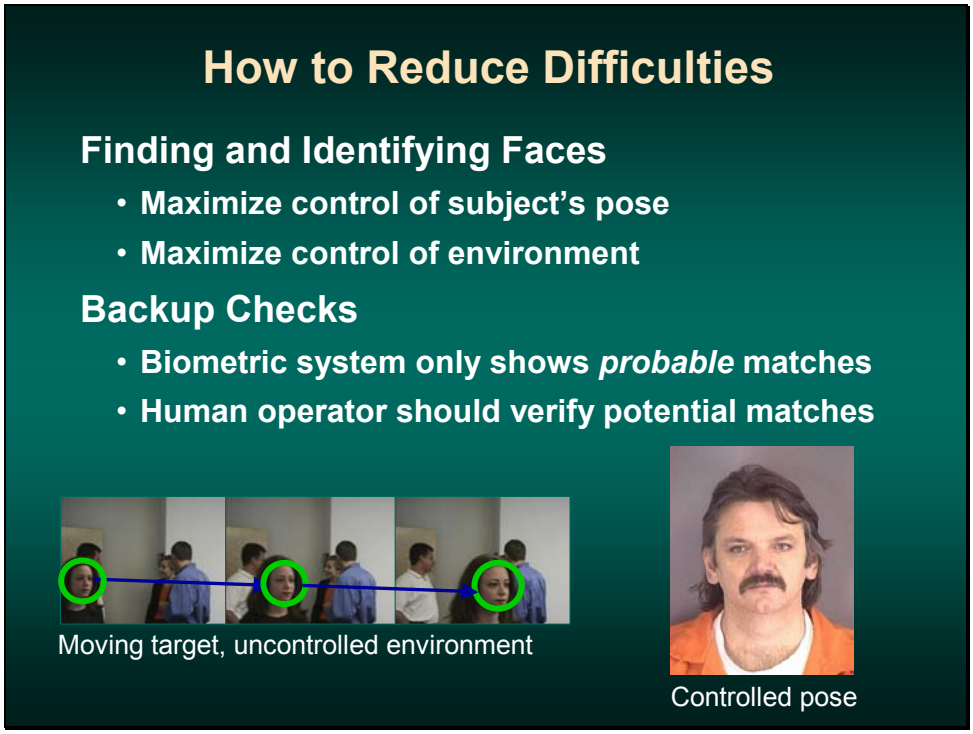
Considerable evidence supports this claim. For example, in a British study, trained supermarket cashiers were tested on their ability to screen shoppers using credit cards that included a photograph of the card owner. Each shopper was issued four cards: one with a recent picture of the shopper, one that included minor modifications to the shopper's hairstyle, facial hair or accessories (*e.g.*, glasses, hat), another card with a photograph of a person similar in appearance to the shopper, and the last card with a photograph of a person who was only of the same sex and race as the shopper. When the various cards were presented to the checkout clerks, more than half of the fraudulent cards were accepted. The breakdown was as follows: 34 percent of the cards that did not look like the shopper were accepted, 14 percent of the cards where the appearance had been altered were accepted, and 7 percent of the unchanged cards were rejected by the clerks.

In addition to unfamiliar face recognition problems, the ability of human beings to detect critical signals drops rapidly from the start of a task, and stabilizes at a significantly lower level within 25 to 35 minutes. Thus the ability of people to focus their attention drops significantly after only half an hour.

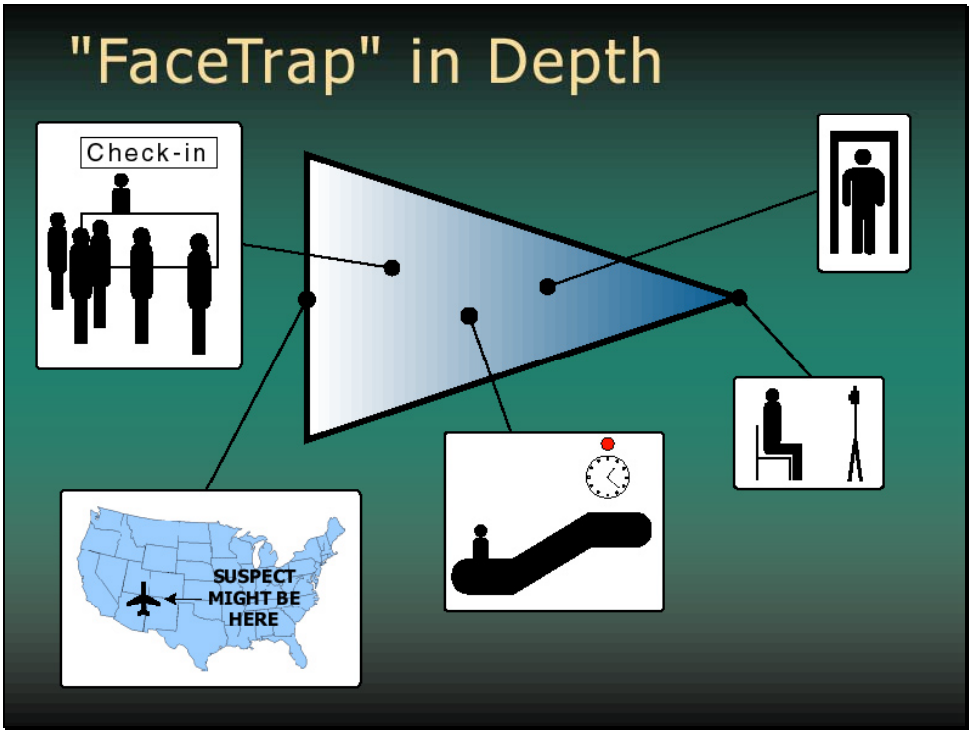


Machines also experience difficulties when they perform facial recognition in a surveillance or watch post scenario. Dr. James L. Wayman, a leading biometrics expert, has explained that performing facial recognition processes with relatively high fidelity and at long distances remains technically challenging for automated systems. At the most basic level, detecting whether a face is present in a given electronic photograph is a difficult technical problem. Dr. Wayman has noted that subjects should ideally be photographed under tightly controlled conditions. For example, each subject should look directly into the camera and fill the area of the photo for an automated system to reliably identify the individual or even detect his face in the photograph. Thus, while the technology for facial recognition systems shows promise, it is not yet considered fully mature.

The "Facial Recognition Vendor Test 2000" study makes clear that the technology is not yet perfected. This comprehensive study of current facial recognition technologies, sponsored by the Department of Defense (DoD) Counterdrug Technology Development Program Office, the Defense Advanced Research Projects Agency (DARPA), and the National Institute of Justice, showed that environmental factors such as differences in camera angle, direction of lighting, facial expression, and other parameters can have significant effects on the ability of the systems to recognize individuals.

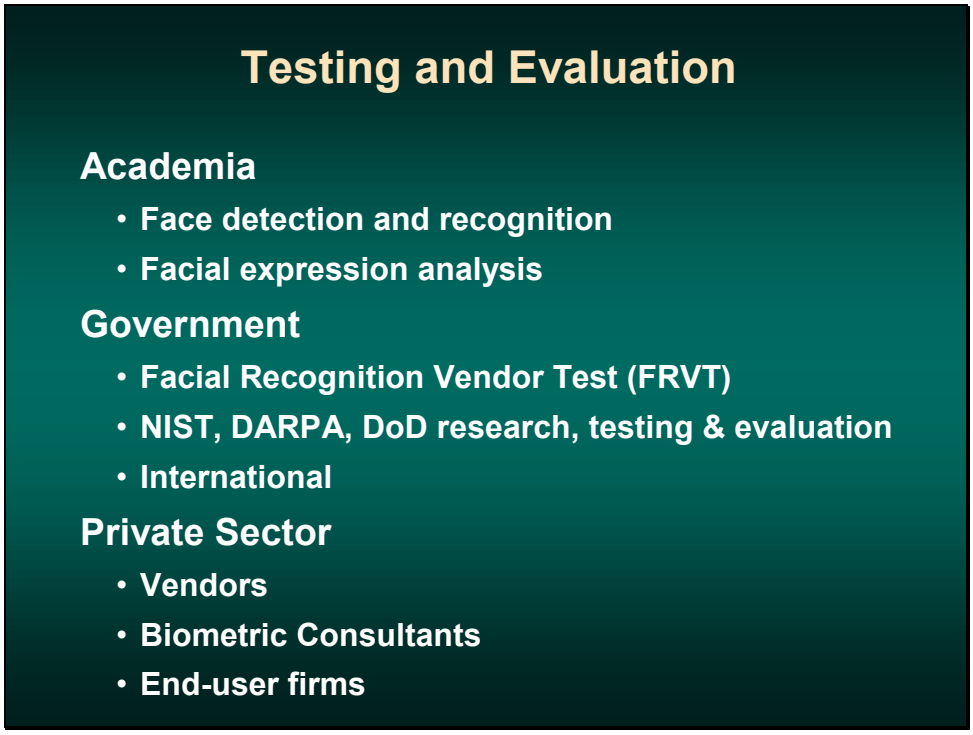


By controlling a person's facial expression, as well as his distance from the camera, the camera angle, and the scene's lighting, a posed image minimizes the number of variables in a photograph. This control allows the facial recognition software to operate under near ideal conditions – greatly enhancing its accuracy. Similarly, using a human operator to verify the system's results enhances performance because the operator can detect machine-generated false alarms.



An "obvious" point that needs stating: The better the quality of the captured image and the database images, the better the facial recognition system will perform.

The "facetrap" triangle above demonstrates this point, with respect to acquiring high-quality images of the target's face. It is difficult to acquire an image if the authorities only know that a suspect might be at an airport west of the Mississippi River. It is easier to capture the image at a facetrap. For example, a surveillance camera can more easily capture images of people at the check-in counter. Sometimes facetraps can be designed to take advantage of people's inclinations. For example, a person going up an escalator will naturally look at a red flashing light above a clock at the top of the escalator. A surveillance camera located there can easily capture an image; the face has been trapped. A camera located at a metal detector also takes advantage of a facetrap. The best facetrap is the one shown at the apex of the triangle—an image captured under tightly controlled conditions.

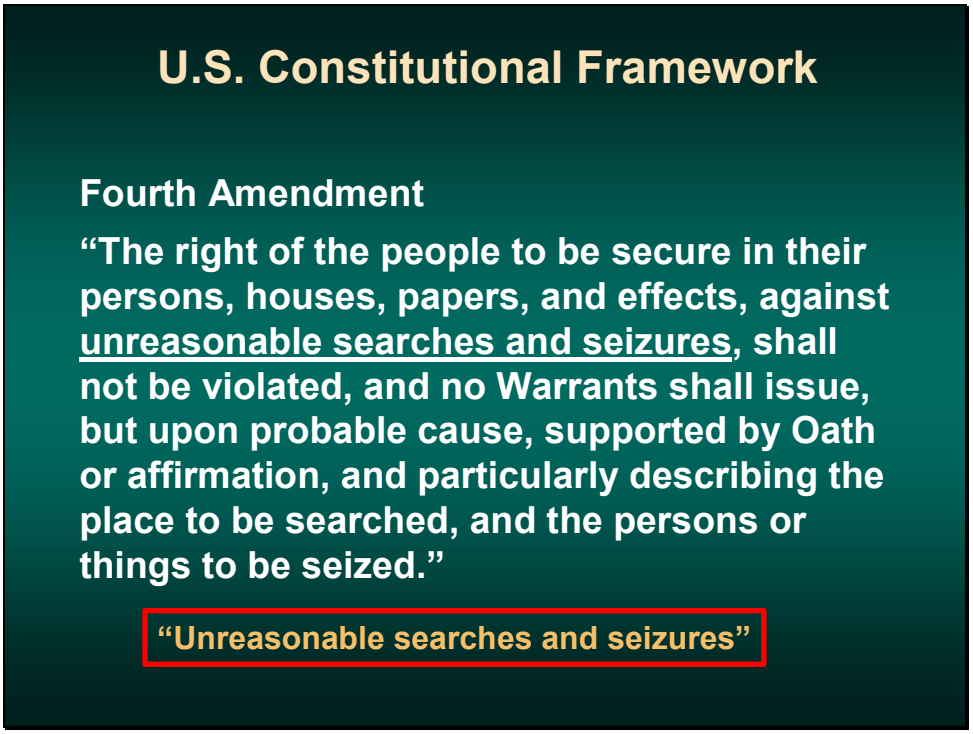


The following factors need to be considered with respect to testing and evaluation of facial recognition systems:

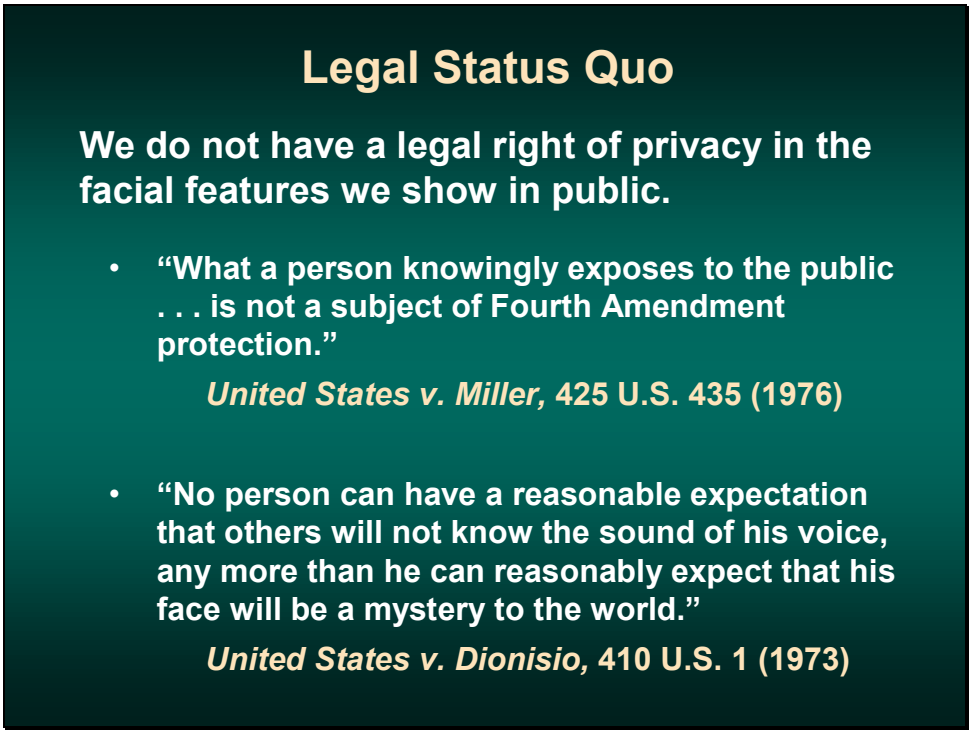
1. Testing should be conducted by independent organizations that will not reap any benefits should one system outperform another (*i.e.* no conflicts of interest involved). The Facial Recognition Vendor Test (FVRT) testing which government agencies sponsor is likely to be very objective.
2. The test philosophy must be considered. For example, the FVRT tries to make the test neither too difficult nor too easy, as it does not want all the systems' performance to cluster at one end of the spectrum. The FVRT also wants to distinguish performance of systems and give feedback to designers for improvement. But a drawback here is that real life data does not present itself this way. Performance in real life may very well prove that none of the systems are useful.
3. Vendors and developers should not know test data beforehand; otherwise, they may be tempted to fine-tune their technology's performance to the specific test data. Performance data that has been fine-tuned to specific test data is not representative of the general performance of the technology being tested.
4. Testing and evaluation should be repeatable. That is, statistically similar results should be able to be reproduced.

In the final analysis, real life deployments will be the ultimate tests of FR systems. For now the jury is still out on the effectiveness of facial recognition systems, however, the technology is improving. Facial recognition systems may yet become a part of our daily lives as they improve and if they become more acceptable, much as CCTV or surveillance camera systems have become.

DISCUSSION OF LEGAL STATUS QUO



Does the use of facial recognition technology violate legally protected privacy rights? Although the words "right to privacy" do not appear in the U.S. Constitution, the concern with protecting citizens against government intrusions in their private sphere is reflected in many of the Constitution's provisions. For example, the First Amendment protects freedom of expression and association as well as the free exercise of religion, the Third Amendment prohibits the quartering of soldiers in one's home, the Fourth Amendment protects against unreasonable searches and seizures, the Fifth Amendment protects against self-incrimination, and the Due Process Clause of the 14th Amendment protects certain fundamental "personal decisions relating to marriage, procreation, contraception, family relationship, child rearing, and education." (*Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833, 851 (1992).) The constitutional "right to privacy" therefore reflects concerns not only for one's physical privacy – the idea that government agents cannot barge into one's home – but also concerns less tangible interests – the idea that citizens should be able to control certain information about themselves and to make certain decisions free of government compulsion. Moreover, the Supreme Court has cautioned 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." (*Whalen v. Roe*, 429 U.S. 589, 605 (1977).)



The use of biometric facial recognition potentially implicates both types of privacy interests. In the context of law enforcement's use of biometric facial recognition to monitor public places, however, it does not appear that such use would run afoul of the protections afforded by the U.S. Constitution.

Some civil libertarians argue that facial recognition is a type of mass, dragnet scanning that is improper, and that law enforcement must have individualized, reasonable suspicion that criminal activity is afoot before it can "search" a subject's face to see if it matches that of an individual in the database. Under current law, however, the type of facial recognition used by law enforcement to monitor public places would almost certainly be constitutional. The United States Supreme Court has explained that government action constitutes a search where it invades a person's reasonable expectation of privacy. But the Court has found that a person does not have a reasonable expectation of privacy in those physical characteristics that are constantly exposed to the public, such as one's facial characteristics, voice, and handwriting. (*United States v. Dionisio*, 410 U.S. 1, 14 (1973).)

So although the Fourth Amendment requires that a search conducted by government actors be "reasonable," which generally means that individualized suspicion is required, a scan of people's facial characteristics as they walk on public streets does not constitute a search. As for information privacy concerns, assuming that law enforcement officials limited their actions to simply comparing scanned images of people in a public area with the computerized

database of suspected terrorists, known criminals, and other legitimate law enforcement targets, then information privacy concerns would likely not arise.

CONCLUSIONS

Biometric facial recognition has the potential to provide significant benefits to society. At the same time, the rapid growth and improvement in the technology could threaten individual privacy rights. The concern with balancing the privacy of the citizen against the government interest occurs with almost all law enforcement techniques. Current use of facial recognition by law enforcement does not appear to run afoul of existing constitutional or legal protections.

Facial recognition is by no means a perfect technology and much technical work has to be done before it becomes a truly viable tool to counter terrorism and crime. But the technology is getting better and there is no denying its tremendous potential. In the meantime, we, as a society, have time to decide how we want to use this new technology. By implementing reasonable safeguards, we can harness the power of the technology to maximize its public safety benefits while minimizing the intrusion on individual privacy.

APPENDIX

Background: The legislation, known as House Bill No. 454, passed the Virginia House of Delegates by a vote of 74-25 earlier in 2002. It is now pending in the Senate Courts of Justice Committee while the Virginia State Crime Commission examines it.

HOUSE BILL NO. 454
AMENDMENT IN THE NATURE OF A SUBSTITUTE
(Proposed by the House Committee on Militia, Police and Public Safety)
(Patron Prior to Substitute--Delegate Griffith)
House Amendments in [ ] -- February 11, 2002

A BILL to amend the Code of Virginia by adding in Title 19.2 a chapter numbered 6.1, consisting of sections numbered 19.2-70.4 through 19.2-70.7, relating to warrants; facial recognition technology.

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 19.2 a chapter numbered 6.1, consisting of sections numbered 19.2-70.4 through 19.2-70.7, as follows:

CHAPTER 6.1.
ORDERS FOR FACIAL RECOGNITION TECHNOLOGY.

§ 19.2-70.4. Definition.

As used in this chapter, "facial recognition technology" means any technology or software system [*that identifies humans by using a biometric system to identify and analyze a person's facial characteristics and is*] *employed for the purpose of matching a facial image captured by cameras placed in any public place, other than in a state or local correctional facility as defined in § 53.1-1, with an image stored in a database.*

§ 19.2-70.5. Who may apply for order authorizing facial recognition technology.

A. Except as provided in subsection A of § 19.2-70.7, no locality or law-enforcement agency shall employ facial recognition technology prior to complying with all of the provisions of this chapter.

B. The Attorney General or his designee, in any case where the Attorney General is authorized by law to prosecute or pursuant to a request in his official capacity of an attorney for the Commonwealth in any city or county, or an attorney for the Commonwealth, may apply to the circuit court, for the jurisdiction where the proposed facial recognition technology is to be used, for an order authorizing the placement of facial recognition technology by any law-enforcement agency in the jurisdiction, when

the technology may reasonably be expected to provide (i) evidence of the commission of a felony or Class 1 misdemeanor, (ii) a match of persons with outstanding felony warrants, (iii) a match of persons or class of persons who are identifiable as affiliated with a terrorist organization, or (iv) a match of persons reported to a law-enforcement agency as missing.

§ 19.2-70.6. Application for and issuance of order authorizing use of facial recognition technology; contents of order; introduction in evidence of information obtained.

A. Each application for an order authorizing the use of facial recognition technology shall be made in writing upon oath or affirmation to the circuit court and shall state the applicant's authority to make the application. Each application shall be verified by the applicant to the best of his knowledge and belief and shall include the following information:

1. The identity of the applicant and the law-enforcement agency;

2. A full and complete statement of the facts and circumstances relied upon by the applicant in support of his request that an order be issued, including, but not limited to, (i) details either as to the particular offenses that have been, are being or are about to be committed, or the event or appearance that would attract individuajos affiliated with a terrorist organization; (ii) a specific description of the nature and location of the facilities where or the place from which the facial recognition technology is to be used; (iii) a description of the type of match being sought; (iv) the identity of any persons or class of persons sought by the use of facial recognition technology as provided in subsection B of § 19.2-70.5; and (v) a description of the type of facial recognition technology to be used and a description of the contents of the database;

3. A statement of the period of time for which facial recognition technology is required to be maintained. However, in no case shall any request for an order granting the use of facial recognition technology be for longer than a period of ninety days;

4. A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to the court for authorization to use facial recognition technology involving any of the same persons, facilities or places specified in the application, and the action taken by the court on each application; and

5. Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the use of facial recognition technology, or a reasonable explanation of the failure to obtain the expected results.

The court may require the applicant to furnish additional testimony or documentary evidence in support of the application.

B. If the court determines on the basis of the facts submitted that the provisions of this chapter have been met, and upon submission of a proper application, the court shall enter

an order, as requested or as modified, authorizing the use of facial recognition technology within the territorial jurisdiction of the court. The application and any order granted or denied may be sealed by the court.

C. Each order authorizing the use of facial recognition technology shall specify:

1. The identity of any persons or class of persons who are the object of the use of the facial recognition technology, or the expected evidence of the commission of felonies or Class 1 misdemeanors from the use of the facial recognition technology;

2. The nature and location of the facilities as to which, or the place where, authority to use facial recognition technology is granted;

3. A description of the type of facial recognition technology to be used;

4. A description of the contents of the database;

5. The name of the agency authorized to use the facial recognition technology;

6. The requirement that only the agency named shall use the facial recognition technology;

7. The period of time, not to exceed ninety days, during which the use of the facial recognition technology is authorized, including a statement that the use shall be terminated at the end of the time period specified, unless the agency applies for and is granted an extension;

8. If the court deems it appropriate, the submission of reports at specified intervals to the court that issued the order, showing what progress has been made toward achievement of the authorized objective and the need for continued use of the facial recognition technology; and

9. The requirement that any facial image captured that is not relevant to (i) evidence of the commission of a felony or Class 1 misdemeanor, (ii) a match of persons with outstanding felony warrants, (iii) a match of persons or class of persons who are identifiable as affiliated with a terrorist organization, or (iv) a match of persons reported to a law-enforcement agency as missing shall be disposed of as soon as possible, but in no event be retained for more than ten days.

D. No order entered under this section may authorize the use of facial recognition technology for any period longer than ninety days from the time the facial recognition technology is operational. Extensions of an order may be granted in accordance with subsection A. The period of extension shall be no longer than the court deems necessary to achieve the purposes for which it was granted and in no event shall the extension be for longer than sixty days.

E. Any violation of the provisions of this subsection may be punished as contempt of court.

§ 19.2-70.7. Certain exemptions from chapter.

A. The provisions of this chapter shall not apply to security measures undertaken at (i) public-use airports in the Commonwealth or (ii) harbors and seaports of the Commonwealth.

B. Any information acquired through facial recognition technology prior to July 1, 2002, shall be admissible in evidence in any suit, action or proceeding.

SELECTED BIBLIOGRAPHY

Blackburn, D. M., "Evaluating Technology Properly: Three Easy Steps to Success," *Corrections Today*, July 2001.

Blackburn, D. M., M. Bone, and P. J. Philips, Ph.D., *Facial Recognition Vendor Test 2000: Evaluation Report,* available at http://www.frvt.org/

Davies, Graham and Sonya Thasen, "Closed-Circuit Television: How Effective an Identification Aid?" *British Journal of Psychology*, 91:3 Aug. 2000.

Hitchcock, E.M., W. N. Dember, J. S. Warm, B. W. Moroney and J.E. See, "Effects of Cueing and Knowledge of Results on Workload and Boredom in Sustained Attention," *Human Factors,* 41:3 Sep. 1999.

Phillips, P.J., et al, "The FERET Evaluation" in H. Wechsler, et al (eds), *Face Recognition: From Theory to Applications,* Berlin, Springer-Verlag, 1998.

Phillips, P.J, "The FERET Database and Evaluation Procedure for Face-Recognition Algorithms," *Image and Vision Computing Journal*, 16.5, 1998.

Phillips, P. J., Alvin Martin, C.L. Wilson, and Mark Przybocki, "An Introduction to Evaluating Biometric Systems," *Computer,* Feb. 2000.

Pike, G., R. Kemp, and N. Brace, "The Psychology of Human Face Recognition," *IEE Electronics and Communications: Visual Biometrics,* 00/018 (2000).

Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833 (1992).

United States v. Dionisio, 410 U.S. 1 (1973).

Warm, J. S. (ed.), *Sustained Attention in Human Performance*, Chichester, England: Wiley, 1984.

Wayman, J. L., *Fundamentals of Biometric Technologies*, available at http://www.engr.sjsu.edu/biometrics/publications_tech.html

Wayman, J. L., "Technical Testing and Evaluation of Biometric Identification Devices" in A. Jain, et al (eds.), *Biometrics: Personal Identification in a Networked Society*, Boston, Kluwer Academic Press, 1999.

Whalen v. Roe, 429 U.S. 589 (1977).

Woodward, John D., Jr., Katharine W. Webb, Elaine M. Newton, et al., *Army Biometric Applications: Identifying and Addressing Sociocultural Concern,* Santa Monica, CA: RAND, MR-1237-A, 2001.

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.