Volume 48 | Issue 3 Article 6

2003

Every Breath You Take, Every Move You Make, I'll Be Watching You: The Use of Face Recognition Technology

Bridget Mallon

Comment

"EVERY BREATH YOU TAKE, EVERY MOVE YOU MAKE, I'LL BE WATCHING YOU"[1]: THE USE OF FACE RECOGNITION TECHNOLOGY

I. INTRODUCTION

Imagine a day in the not too distant future when you go to Big Brother Corporation to apply for a job. After filling out an application, submitting a resume and the requisite references, you are granted an interview. After spending the morning meeting with various employees of the Corporation, you are told that unfortunately, they will be unable to hire you. When you inquire as to why, you are informed that the employer does not feel you are suited to work at Big Brother Corporation. As it turns out, while you were being interviewed, a camera in the office took a digital photograph of you that was then scanned through a database of mug shots and driver's license photographs. Your photograph was matched with the photo from your driver's license, pulling up your entire history: any police record, credit history, medical history, even a list of items you have purchased with your credit card. Based on your personal record, they are convinced you are not suited for employment with Big Brother Corporation.

While such a scenario, on its face, appears improbable, it now seems that George Orwell's fears for the future, once thought of as far fetched, have become a reality.[2] Recent technological innovations have made it possible to not only instantly recognize individuals, but also to track their movements and recall their entire history within seconds.[3] The use of face

1. THE POLICE, *Every Breath You Take*, *on* SYNCHRONICITY (A&M Records 1983).

2. *See generally* GEORGE ORWELL, 1984 (Reprint ed. 1990) (referring to concept of book). In Orwell's 1949 novel, he flashes forward to a future when Big Brother monitors your every move. *See generally id.* (describing background of novel). The notion that video monitoring devices would be present everywhere seemed inconceivable at the time the book was published; however, given the recent advances in technology, Orwell's scenario seems more real than ever. *See* Grayson Barber, *Living on the Wrong Side of a One-Way Mirror: Face Recognition Technology and Video Surveillance*, ChipCenter-QuestLink, *at* http://www.chipcenter.com/columns/COL_20010718.html (July 18, 2001) (noting Orwell's portrayal of "the condition of life in a tyrannical police state"); Agnes Blum, *Beach Surveillance Plan Gets More Critics*, VIRGINIAN PILOT & LEDGER-STAR, *at* http://www.pilotonline.com/news/nw0711nay.html (July 11, 2001) (observing that proposal to use face recognition technology has "Orwellian overtones").

3. *See generally* Robert O'Harrow Jr., *Matching Faces with Mug Shots*, WASH. POST, Aug. 1, 2001, at A1 (recognizing advancements in technology); Charles Piller, et al., *Criminal Faces in the Crowd Still Elude Hidden ID Cameras*, L.A. TIMES, Feb. 2, 2001, at A1 (same); Kathleen Ellis, *ID Them By the Way They Walk*, WIRED NEWS (Sept. 15, 2000), *at* http://www.wired.com/news/print/0,1294,38775,00.

recognition technology, introduced to the world during the 2001 Super Bowl, is rapidly expanding in the wake of growing security concerns, stemming from the events of September 11, 2001.[4]

This Comment focuses on facial recognition technology and the privacy problems that arise from its use. Because this technology is just emerging from its developmental stages, its legality remains untested in court.[5] Although the government's use of this technology appears to fall within Constitutional bounds, its use by third parties may pose more of a threat.[6] Part II of this Comment discusses how facial recognition technology works, as well as how it has been used in the past.[7] With the expanding use of this technology, it is important to examine its potential legal implications.[8] Part III briefly discusses the history of privacy in public places.[9] Part IV analyzes the United States Supreme Court's treatment of privacy in public places and its application to the use of facial recognition technology.[10] Finally, Part V discusses the future use of facial recogni-

---

html (same); Julia Scheeres, *Smile, You're on Scan Camera*, WIRED NEWS (Mar. 14, 2001), *at* http://www.wired.com/news/print/0,1294,42317,00.html. (same).

4. *See generally* Editorial, *Digital Big Brother*, ST. LOUIS POST-DISPATCH, Feb. 5, 2001, at C18 (noting use of face recogniation technology at 2001 Super Bowl); Mary Huhn, *Just a Face in the Crowd?—Superbowl Kicked Off the Use of Face Recognition Software—but Is this an Invasion of Privacy?*, N.Y. POST, June 26, 2001, at 51 (same); Martin Kasindorf, *'Big Brother' Cameras on Watch For Criminals*, USA TODAY, Aug. 2, 2001, at A3 (same); Peter Slevin, *Police Video Cameras Taped Football Fans; Super Bowl Surveillance Stirs Debate*, WASH. POST, Feb. 1, 2001, at A1 (same); Robert Trigaux, *Cameras Scanned Fans for Criminals*, ST. PETERSBURG TIMES, Jan. 31, 2001, at 1A (same); Kevin Anderson, *Anger over Face-Scanning Cameras*, BBC News (Aug. 20, 2001), *at* http://news.bbc.co.uk/1/hi/sci/tech/1500017.stm (same); *On January 28th, Criminals no Longer Another Face in the Tampa Stadium Crowd*, Viisage Tech., Inc., *at* http://www.viisage.com/january_29_2001.htm (Jan. 29, 2001) (same).

5. *See* Barber, *supra* note 2, at http://www.chipcenter. com/columns/COL_20010718.html (noting surveillance remains untested in court); Kenneth P. Nuger, *Biometric Applications: Legal and Societal Considerations*, Nat'l Biometric Test Ctr. (2001), *at* http://www.engr.sjsu.edu/biometrics/publications_consideration.html (commenting that this new technology has yet to be addressed in court).

6. *See* Nuger, *supra* note 5, at http://www.engr.sjsu.edu/ biometrics/publications_consideration.html (recognizing that privacy issues arise from third party use of biometrics); Janelle K. Prevost, *Biometrics with Limited Government Intervention: How to Provide for Privacy and Security Requirements of Networked Digital Environments*, MIT ETHICS & L. ON ELEC. FRONTIER (Fall 1999), *at* http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.html (analyzing various privacy problems arising from use of new technology).

7. For a further discussion of how face recognition technology works and its use, see *infra* notes 12-72 and accompanying text.

8. For a further discussion of the legality of the use of face recognition technology, see *infra* notes 110- 47 and accompanying text.

9. For a further discussion of the history of privacy in public places, see *infra* notes 73-109 and accompanying text.

10. For a further discussion of the privacy issues that arise from the use of face recognition technology, see *infra* notes 111-48 and accompanying text.

tion technology and electronic surveillance in light of growing security fears throughout the United States and the world.[11]

II. USE OF FACIAL RECOGNITION TECHNOLOGY

A. *Biometrics—An Introduction*

Biometrics refers to the way in which humans can be identified by the unique characteristics of their bodies.[12] Currently, humans are identified in many ways, including fingerprints and facial features,with the most common form quickly becoming face recognition.[13] Although fingerprints and faces are the most common forms of biometric identifiers, they are certainly not the only ones.[14] Scientists are currently working on numerous forms of identification, hoping to one day reach the goal of identifying individuals wherever they go, even up to a half mile away.[15]

---

11. For a further discussion of the future use of face recognition technology, see *infra* notes 148-78 and accompanying text.

12. *See Biometrics Introduction*, Axis Tech, *at* http://www.axistech.com (last visited Aug. 29, 2002) (defining biometrics); Beth Givens, *Privacy Today: A Review of Current Issues*, Privacy Rights Clearinghouse (Mar. 2001), *at* http://www.privacyrights.org/ar/Privacy-IssuesList.htm (same); Ross Kerber, *Face Off*, BOSTON GLOBE ONLINE (Aug. 20, 2001), *at* http://www.digitalmass.boston.com/companies/globe_profiles/2001/08/viisage2.html (same); William W. Wilson, *Letter Regarding CA Legislation*, Int'l Biometric Indus. Ass'n (June 18, 2001), *at* http://www.ibia.org/calegletter061801.htm (same).

13. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (identifying fingerprints and facial features as two forms of biometric identification); Givens, *supra* note 12, at http://www.privacyrights.org/ar/Privacy-IssuesList.htm (listing forms of biometric identification). Face recognition technology takes two forms: surveillance and identification. *See* Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (describing types of face recognition technology). Although there are, undoubtedly, a number of privacy issues that surround the use of this technology for surveillance, this Comment will focus mainly on its use for identification purposes.

14. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (describing forms of biometric identification); Givens, *supra* note 12, at http://www. privacyrights.org/ar/Privacy-IssuesList.htm (discussing types of biometric identification). The number of characteristics used to identify individuals is rapidly growing. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com/ (examining "human traits that can be used in biometrics"). Currently, humans are being identified by their fingerprints, voice, face, retina, iris, handwriting, hand geometry, finger geometry, palm recognition and signature recognition. *See id.* (listing types of biometric identification). Each of these different forms of recognition works in its own way to create a specific and unique map of the personal characteristic that is then matched against a database in search of a match. *See id.* (noting mechanics of biometric technology).

15. *See* Ellis, *supra* note 3, *at* http://www.wired.com/news/print/0,1294,38775,00.html (discussing plans for future forms of identification). At the Biometric Consortium 2000 Conference, co-sponsored by the National Security Agency, researchers unveiled a new software program designed to identify individuals by the way they walk. *See id.* (discussing new program). This new technology is designed to "isolat[e] . . . a 'signature of human motion'" and allow individuals to be identified by the way they walk, thereby working even if an individual's face is not visible to the surveillance cameras. *See id.* (detailing potential capabilities of

Face recognition technology works by creating a "map" of the face from a photograph that a surveillance camera takes.[16] Each face has eighty distinctive points that are recorded from the photograph.[17] Once these distinctive points are mapped, they are translated into a unique set of numbers, using a sophisticated algorithm, from which a face map is created.[18] Once this map is created, it is scanned through a database of stored face maps.[19] Only fourteen to twenty-two points need to line up in order to make a match.[20] If the computer program signals a match, the original photograph and the photograph it was matched with are displayed side by side on a screen.[21] Then, whoever is monitoring the

---

system). Other identification systems under development include an effort to install an electronic pen and pad system onto personal computers that would allow individuals to develop a unique signature that establishes their identities. *See id.* (explaining other forms of identification on display at Biometric Consortium).

16. *See* O'Harrow, *supra* note 3, at A1 (discussing ability to map facial features); Editorial, *Owens' Balancing Act*, DENVER POST, July 20, 2001, at B6 (revealing that computer program creates map of individual's face).

17. *See Face Recognition Technology is Next—Big Brother Arrives*, BOSTON GLOBE, Mar. 1, 2000, at A15 (explaining how face recognition technology works); Kasindorf, *supra* note 4, at A3 (detailing mechanics of face recognition technology).

18. *See* Kasindorf, *supra* note 4, at A3 (identifying measurement of facial characteristics as method of new technology); Piller et al., *supra* note 3, at A1 (detailing how facial scans work); John D. Woodward, Jr., *And Now, the Good Side of Facial Profiling*, WASH. POST, Feb. 4, 2001, at B4 (discussing measurement of distance and angles of face to map face); Anderson, *supra* note 4, at http://news.bbc.co.uk/1/hi/sci/tech/1500017.stm (examining how facial scans take facial features and transform them into numerical codes); *Facial Recognition*, Viisage Tech., *at* http://www.viisage.com/facialrecog.htm (last visited Aug. 31, 2002) (discussing mechanics of technology); Scheeres, *supra* note 3, *at* http://www.wired.com/news/print/0,1294,42317,00.html (noting use of "numerical codes" to map faces).

19. *See* Kasindorf, *supra* note 4, at A3 (defining method of technology); O'Harrow, *supra* note 3, at A1 (mentioning use of stored database of images); *ACLU Probes Police Use of Facial-Recognition Surveillance Cameras in Florida City*, Am. Civil Liberties Union (July 6, 2001), *at* http://www.aclu.org/news/2001/n070601a.html (describing process of face recognition).

20. *See Face Recognition Technology is Next—Big Brother Arrives*, *supra* note 17, at A15 (explaining how face recognition technology matches points in order to identify someone); Piller et al., *supra* note 3, at A1 (detailing process of matching faces).

21. *See Face Recognition Technology is Next—Big Brother Arrives*, *supra* note 17, at A15 (discussing what happens when computer signals match); Slevin, *supra* note 4, at A1 (stating that apparent matches were "flashed side by side onto a computer screen"). This is not the only method of face recognition technology. *See* Piller et al., *supra* note 3, at A1 (discussing methods of face recognition). Another form of technology involves taking a photograph of the face and then developing a faceprint by measuring the size of an individual's facial features. *See id.* (identifying different methods of matching faces). Calculating the width of a nose or the space between the eyes can provide a more accurate means of face recognition because these measurements do not change, even if the individual ages, gains weight or grows facial hair. *See id.* (describing capabilities of system to account for changes in appearance).

screens, either police or security, decides whether or not the faces are actually a match.[22]

This technology was formulated in the early 1990s with a Department of Defense (DOD) initiative called the FERET Program.[23] The program was designed to determine whether it would be possible to use algorithms accurately to measure human faces.[24] The government allocated $6.5 million to several universities that were enlisted to assist in the program.[25]

22. *See* Slevin, *supra* note 4, at A1 (stating once potential match was found police had to determine whether match was accurate). Biometric technology serves two main functions: identification and verification. *See Biometrics Introduction, supra* note 12, at http://www.axistech.com (detailing function of biometric technology). Identification is the process by which an individual's photograph is scanned through a database of photos (criminals, runaways, etc.) in search of a match. *See id.* (stating purpose of identification systems). Verification is the method by which an individual's photograph is scanned through a database of stored users. *See id.* (noting purpose of verification systems). Verification is often employed by businesses who use the technology to identify their employees. *See id.* (detailing use of verification technology by numerous corporations).

23. *See* O'Harrow, *supra* note 3, at A1 (indicating facial recognition technology began through DOD initiative); Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (identifying FERET program as beginning of serious research in face recognition).

24. *See* Dep't of Def., *FERET Overview*, Dep't of Def. Counterdrug Tech. Dev. Program Office, *at* http://www.dodcounterdrug.com/facialrecognition/Feret.feret.htm (last visited Oct. 2, 2002) (delineating steps and purpose of FERET program). The DOD Counterdrug Technology Development Program Office began the FERET program in September 1993 with the goal of developing "automatic face recognition capabilities that could be employed to assist security, intelligence, and law enforcement personnel in the performance of their duties." *Id.*

25. *See id.* (noting government funding of program). The program had three main elements: sponsorship of the research, collecting a database and performing evaluations. *See id.* (listing steps taken in FERET program). Once the participating groups were chosen, the FERET database of images was formed between August 1993 and July 1996, consisting of 14,126 images, including 1199 individuals and 365 duplicate images. *See id.* (detailing formation of database). For some of the duplicate images, over two years had passed between the first photograph and the second, allowing researchers to study the effect that changes in an individual's appearance could have. *See id.* (allowing for changes in appearance to measure accuracy of system).

While the database was being compiled, the individual research groups were working on developing their algorithm-based programs. *See id.* (discussing work of individual groups involved in program). All of the groups receiving funding were required to participate in a number of evaluations. *See id.* (detailing purpose and content of individual evaluations). The first set of evaluations, in August 1994 were designed to measure the ability of the algorithms to accurately identify individuals' faces in a database. *See id.* (stating goal of evaluation was to measure ability of system to "automatically locate, normalize, and identify faces"). In March 1995, the second set of evaluations measured the algorithms in a larger database of images. *See id.* (observing expanded database was used for second evaluation). The final set of evaluations took place in September 1996 and consisted of a full set of performance tests that measured the ability of the algorithms to identify individuals in a number of different situations. *See id.* (discussing final evaluation procedure for systems).

The program concluded in 1998, with private corporations waiting anxiously to capitalize on the new technology.[26] Subsequently, in November 2000, the DOD initiated the Human ID at a Distance program.[27] This new program was an effort by the government to develop technology that could not only identify humans, but could identify "'humans alone, or in groups, from great distances' and in the dark."[28]

---

26. *See id.* ("Many of the algorithms that took part in FERET form the foundation of today's commercial systems."). The FERET program was officially completed in 1998 and program funding totaled over $6.5 million. *See id.* (summarizing FERET progam). The FERET program was one of the first to demonstrate the viability of using algorithm-based systems to identify individuals, thus leading to the development of many of the current face recognition systems. *See id.* (noting importance of FERET program).

27. *See* Kasindorf, *supra* note 4, at A3 (explaining Human ID program); O'Harrow, *supra* note 3, at A1 (stating program is part of "anti-terrorism initiative"); Woodward, *supra* note 18, at B4 (observing that Human ID program began in response to terrorist attack on Khobar Towers).

28. *See* Dep't of Def., *FERET Overview*, *supra* note 24, at http://www.dodcounterdrug.com/facial recognition/Feret.feret.htm (examining new DOD initiatives); *Human ID at a Distance*, Information Awareness Office, *at* http://www.darpa.mil/iao/HID.htm (last visited Oct. 2, 2002) (detailing Human ID program). The Human ID at a Distance program is a four year program that picks up where the FERET program left off and is designed to improve the capabilities of a number of biometric systems. *See* Dep't of Def., *FERET Overview*, *supra* note 24, at http://www.dodcounterdrug.com/facial recognition/FERET.feret.htm (noting purpose of program). The DOD is spending $50 million to improve the accuracy of biometrics and increase the ability of technology to identify "non-cooperative subjects." *See id.* (same). The system would be designed to operate at all times of day and would "automatically create folders for collecting data on repeat visitors." *See Human ID at a Distance*, *supra*, at http://www.darpa.mil/iao/HID.htm (explaining automatic features of Human ID system). With the dramatic expectation for the new program, there are a number of possible problems that the new program faces. *See id.* (detailing problems associated with new program).

> The challenges facing the Human ID program are:
>
> (1) develop systems to recognize non-cooperative and un-cooperative subjects at a distance of up to 500 feet from the acquisitions sensor(s);
>
> (2) develop systems that identify people from multiple biometrics or sensors by fusing multiple biometrics and switching between different biometric signatures that are designed to function under varying operating conditions, i.e., different lighting or weather conditions;
>
> (3) increase the number of scenarios to which identification technologies can be applied (e.g., notifying authorities when a person appears multiple days at one site or is spotted at different sites and the person is not known to the system); and
>
> (4) advance evaluation methodologies to a point where they establish an identification and surveillance science that will
>
> (a) determine fundamental limits of biometrics,
>
> (b) determine the effects of varying data sets on performance,
>
> (c) establish standard protocols for collecting data sets, evaluating systems, and designing experiments, and
>
> (d) scientifically identify critical factors that affect performance.

Id.

Because of this urge to identify people in groups, from great distances or in the dark, accuracy is one of the most important concerns surrounding this new technology.[29] Face recognition systems are designed to accommodate a variety of changes in facial features while still accurately identifying faces.[30] Any change in age, facial hair, weight or even the presence or absence of glasses should, ideally, not interfere with the program's accuracy.[31]

Nevertheless, despite all attempts to maintain accuracy, the technology is not foolproof.[32] Recent studies have indicated a rather large percentage of error in the new technology.[33] The National Institute of Standards and Technology (NIST) recently conducted a study to measure the accuracy of face recognition systems.[34] According to the results, posed photos of a person, taken only eighteen months apart, were rejected by the system, which indicated no match approximately forty-three percent of the time.[35] An anticipated DOD study is expected to confirm these statistics.[36]

---

29. *See* Piller et al., *supra* note 3, at A1 ("Experts warn that covert digital facial scans can be highly unreliable in public settings . . . ."); Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.htm (admitting "the technology has severe limitations").

30. *See* O'Harrow, *supra* note 3, at A1 (quoting Visionics corporation's claim that "its software is able to account for changes").

31. *See id.* (noting ability of system to maintain accuracy); Piller et al., *supra* note 3, at A1 (observing that certain facial features in adults do not change in response to age, weight gain or other changes).

32. *See* Piller et al., *supra* note 3, at A1 (stating "technology is still far from foolproof"); *see also Frequently Asked Questions,* Identix Inc., *at* http://www.identix.com/newsroom/face_faqs.html (last visited Sept. 15, 2002) (answering frequently asked questions regarding face recognition technology). According to Identix Incorporated, there are four major causes of face recognition failure: glare on eyeglasses that obstructs a clear view of the face, presence of long hair that falls in front of the face and prevents a clear photograph from being taken, poor lighting and a lack of resolution in the photograph, preventing a clear and accurate picture. *See id.* (listing causes of failure).

33. *See* Piller et al., *supra* note 3, at A1 (observing that "digitized photos shot at an angle or in poor light create images that often fail to match existing mug shots").

34. *See id.* (examining testing by NIST).

35. *See id.* (disclosing failure rates of new technology).

36. *See* Dep't of Def., *Facial Recognition Vendor Test 2000 Overview,* Dep't of Def. Counterdrug Tech. Dev. Program Office, *at* http://dodcounterdrug.com/facialrecognition/FRVT2000/frvt2000.htm (last visited Oct. 2, 2002) (summarizing Facial Recognition Vendor Test 2000); Laura Kinsler, *City Council Narrowly Supports Face Scanning,* TBO.com (Aug. 3, 2001), *at* http://www.abatesc.com/news/news-6-aug-01.htm (analyzing accuracy of face recognition technology). From May to June 2000, the DOD performed the Facial Recognition Vendor Test 2000, which was designed to evaluate the capabilities of a number of face recognition systems that are currently available in the United States. *See* Dep't of Def., *Facial Recognition Vendor Test 2000 Overview, supra, at* http://dodcounterdrug.com/facialrecognition/ FRVT2000/frvt2000.htm (last visited Sept. 14, 2002) (detailing Facial Recognition Vendor Test 2000). The test was aimed at aiding government agencies in their search for added security measures, by demonstrating the capabilities of the

The results of face recognition systems can trigger false "matches" or false "rejections" for any number of reasons.[37] For example, bad lighting, the glare of eye glasses, facial hair and the angle at which the photograph is taken can all interfere with the accuracy of the results.[38] Even in controlled circumstances, with posed photos, the results remain less than completely accurate.[39] The inaccuracies are even greater when the photos are taken of random individuals on the street because the surveillance cameras are often not able to take photographs of individuals head on.[40]

---

various systems available. *See id.* (specifying that goal of test was to evaluate available face recognition systems). The test was divided into two parts: the first part was designed to test the ability of all of the algorithm-based systems to see how they perform, the second test allowed each vendor to set up his or her system using the necessary cameras, lighting and other equipment needed for his or her system to perform. *See id.* (detailing format of test). The test used two timed portions to determine the ability of the system to operate accurately under a given set of circumstances. *See id.* (reviewing use of time in order to test accuracy of systems).

The DOD's tests were performed in government labs and under controlled circumstances, however, outside of these controlled circumstances, the accuracy of the systems decreases. *See* Kinsler, *supra*, at http://www.abatesc.com/news/news-6-aug-01.htm (assessing reality of accuracy of system).

37. *See* Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99papers/prevost-biometrics.html (evaluating accuracy of face recognition). Once a face is mapped and scanned through the computer system, there are two possible problems that may arise: false acceptance and false rejection. *See id.* (identifying potential problems with matching). False acceptance occurs when an individual is wrongly matched with a photograph in the system. *See id.* (explaining cause of false acceptance). False rejection occurs when an individual is rejected, even though he or she is an accurate match for someone in the computer database. *See id.* (analyzing cause of false rejection).

38. *See* Piller et al., *supra* note 3, at A1 (recognizing inaccuracies of technology); Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (observing potential for system to be fooled).

39. *See* Piller et al., *supra* note 3, at A1 (citing results of NIST studies). Although face recognition technology remains less than one hundred percent accurate, the developers of the technology are making strides. *See* Visionics, *Visionics Introduces Fourth Generation—G4—FaceIt Engine*, Yahoo! Finance (Oct. 1, 2001), *at* http://biz.yahoo.com/bw/011001/10293_1.html (presenting advances in system's capabilities). Just recently, Visionics unveiled the latest version of their FaceIt software, the software being used in Tampa, Florida. *See id.* (detailing new system). The newest version, G4, has recently completed strict government testing through the Facial Vendor Test 2000. *See id.* (noting performance in Facial Vendor Test 2000). For a complete discussion of the Facial Recognition Vendor Test 2000, see *supra* note 36. The results of the testing prove that Visionics new program is the most effective of all of the systems tested, demonstrating notable improvements in the system's ability to accurately match faces, compensate for poor lighting and generally reduce false alarms. *See* Visionics, *supra*, at http://biz.yahoo.com/bw/011001/10293_1.html (detailing capabilities of newest system).

40. *See* Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (observing inaccuracies of technology).

B. *The 2001 "Snooperbowl"*[41]

The 2001 Super Bowl marked the first time the general public was introduced to the use of face recognition technology.[42] Although previously used in a variety of capacities, the Super Bowl was one of the first times this technology was tested and used on a large scale in the United States.[43] This led a number of individuals concerned with the use of this technology to dub the 2001 Super Bowl the "Snooperbowl."[44]

From January 21 through January 28, 2001, Graphco Technologies, Inc. provided a surveillance and facial recognition system for Tampa's Raymond James Stadium and two other venues hosting Super Bowl related activities.[45] As the 71,000 Super Bowl spectators entered the four main gates of Raymond James Stadium, approximately twenty cameras recorded

---

41. *See generally* Anderson, *supra* note 4, at http://news.bbc.co.uk/hi/english/sci/tech/newsid_1500000/1500017.stm (referring to the 2001 Super Bowl as "Snooperbowl"); Kasindorf, *supra* note 4, at A3 (same).

42. *See* Barbara Dority, *A Brave New World—Or a Technological Nightmare? Big Brother is Watching!*, HUMANIST, May 1, 2001, at 9 (examining events at 2001 Super Bowl); Huhn, *supra* note 4, at 51 ("[Face recognition's] first presence on the worldwide stage kicked off in Tampa, Fla., in January this year at Super Bowl XXXV."); Givens, *supra* note 12, at http://www.privacyrights.org/ar/Privacy-Issues-List.htm (indicating Super Bowl was first time Americans learned of face recognition technology); Julia Scheeres, *Face Scanners Turn Lens on Selves*, WIRED NEWS (July 31, 2001), *at* http:// www.wired.com/news/print/0,1294,45687,00.html (observing that face recognition technology "first gained public notoriety" at Super Bowl).

43. *See* Kerber, *supra* note 12, at http://www.boston.com/dailyglobe2/232/business/Face_offP.shtml (observing "technology was able to jump rapidly from an obscure corner of military-and-security research into the arsenal of a metropolitan police force"); Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (citing previous uses of technology). The system used at the 2001 Super Bowl was created by Graphco Technologies, Inc., however it is not the only company that specializes in this type of technology. *See* Slevin, *supra* note 4, at A1 (quoting Graphco Technologies's managing director). Currently, there are over twenty companies that manufacture facial recognition systems. *See* Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (noting number of companies that produce face recognition systems).

44. *See generally* Kasindorf, *supra* note 4, at A3 (nicknaming 2001 Super Bowl based on use of face recognition technology); Lauren Weinstein, *Be Seeing You!*, 5/1/01 COMM. ACM 128 (May 1, 2001) (same); *ACLU Calls for Public Hearings on Tampa's "Snooper Bowl" Video Surveillance*, Am. Civil Liberties Union (Feb. 1, 2001), *at* http://archive.aclu.org/news/2001/n020101a.html (same); Anderson, *supra* note 4, at http://news.bbc.co.uk/hi/english/sci/tech/newsid_1500000/1500017.stm (same); Jay Lyman, *Critics Blast U.S. Ties to 'Snooper Bowl' Technology*, Yahoo! News (Aug. 1, 2001), *at* http://dailynews.yahoo.com/htx/nf/20010802/tc/12458_1.html (same); Julia C. Martinez, *Owens: Hold Off on Face-ID Technology*, DENVERPOST.COM (July 19, 2001), *at* http://www.denverpost.com/Stories/0,1002,53%257E70770,00.html (same).

45. *See On January 28th, Criminals no Longer Another Face in the Tampa Stadium Crowd*, *supra* note 4, at http://www.viisage.com/january_29_2001.htm (discussing use of Graphco Technologies's system at Super Bowl); *Tampa Uses Cameras to Scan for Wanted Faces*, (July 2, 2001) *at* http://cnn.com/2001/TECH/ptech/07/02/high.tech.security.ap/ (noting presence of system at Super Bowl).

dozens of images.[46] These images were fed into computers and ran against a database of photographs.[47] The same process occurred at two other locations in Tampa where various Super Bowl events occurred.[48]

Prior to the Super Bowl, Tampa police provided Graphco Technologies with a database of 1700 individuals who were convicted of various crimes ranging from ticket scalping to violent crimes.[49] During the event, the system registered nineteen hits, eighteen of which the police decided were false positives.[50] The one hit that the police believed was accurate was an individual who had a history of ticket scalping.[51] By the time an officer was dispatched to find the suspect, however, the suspect had disappeared.[52] This incident demonstrates one of the system's major drawbacks: Although the technology is capable of scanning approximately seventy million images per minute, it still does not operate fast enough to allow the police to immediately identify and approach suspects.[53]

---

46. *See Digital Big Brother*, *supra* note 4, at C18 (reporting presence of 71,000 spectators at Super Bowl); Huhn, *supra* note 4, at 51 (noting presence of cameras at turnstiles); Piller et al., *supra* note 3, at A1 (noting presence of cameras at every turnstile); Anderson, *supra* note 4, at http://www.news.bbc.co.uk/hi/english/ sci/tech/newsid_1500000/1500017.stm (discussing use of cameras at game); Declan McCullagh, *Call it Super Bowl Face Scan I*, WIRED NEWS (Feb. 2, 2001), *at* http://www.wired.com/news/print/0,1294,41571,00.html (last visited Sept. 10, 2002) (explaining how face recognition software secretly scanned every face at 2001 Super Bowl); Trigaux, *supra* note 4, at http://www.sptimes.com/News/013101/news_pf/TampaBay?Cameras_scanned_fans_.shtml (reporting use of twenty-two cameras at Super Bowl).

47. *See Digital Big Brother*, *supra* note 4, at C18 (noting images of fans being scanned); Slevin, *supra* note 4, at A1 (observing scanning of attendees); McCullagh, *supra* note 46, at http://www.wired.com/news/print/0,1294,41571,00.html ("Face-recognition software surreptitiously scanned everyone passing through turnstiles . . . ."); Trigaux, *supra* note 4, at http://www.sptimes.com/News/013101/news_pf?TampaBay? Cameras_scanned_fans_.shtml (discussing how each person entering stadium was photographed).

48. *See On January 28th, Criminals no Longer Another Face in the Tampa Stadium Crowd*, *supra* note 4, at http://www.viisage.com/january_29_2001.htm (noting presence of cameras at stadium and other areas hosting Super Bowl events).

49. *See* Piller et al., *supra* note 3, at A1 (discussing events at 2001 Super Bowl).

50. *See id.* (reporting on matches made); *see also* Editorial, *Super Day for Big Brother*, L.A. TIMES, Feb. 2, 2001, at B8 (noting number of matches at Super Bowl); Slevin, *supra* note 4, at A1 (discussing success of system); *Tampa Uses Cameras to Scan for Wanted Faces*, *supra* note 45, at http://cnn.com/2001/TECH/ptech/07/02/high.tech. security.ap/ (explaining that system made nineteen matches, but there were no arrests).

51. *See* Slevin, *supra* note 4, at A1 (discussing identification of individual at Super Bowl).

52. *See id.* (explaining how suspect disappeared before police could question him).

53. *See* Piller, *supra* note 3, at A1 (noting observations of Professor Doug Tygar). Doug Tygar, University of California, Berkeley professor of computer science noted that "[n]o system works fast enough to immediately apprehend a suspect before that person melts into the crowd." *Id.* Because of the delay between the time a photograph is taken, scanned through the database and a match is made, it will be difficult for police to apprehend suspects. *See id.* (discussing delay

C. *On the Street Where You Live*

Even before its use at the Super Bowl, Tampa officials decided to integrate face recognition technology into their arsenal of crime fighting techniques.[54] Today, as people walk down the streets of Tampa, Florida's historic Ybor City, they are greeted by signs stating "Area Under Video Monitoring."[55] On approximately every block, tall poles support a total of thirty-six surveillance cameras that are constantly swiveling to monitor citizens strolling through the often crowded entertainment district.[56] At a nearby location, police monitor ten video screens and search for matches between faces from the street and those found in a database of felons and runaways.[57] Many Ybor City residents are not pleased with the constant presence of cameras in their hometown.[58] For example, since the cameras installation, demonstrations and questions regarding privacy have

---

resulting in difficulty in apprehension). This technology is designed to be used in places where individuals are not simply standing around, but are constantly moving, thereby making the apprehension of a potential suspect extremely difficult. *See id.* (noting use of technology in commercial arenas).

54. *See* Kerber, *supra* note 12, at http://www.boston.com/ dailyglobe2/232/ business/Face_offP.shtml (noting presence of system, in Tampa, years before use at Super Bowl). Ybor City was chosen as one of the first cities to test out this new technology because a $45 million improvement plan left the city capable of installing the cameras and cables necessary for the system. *See* Logan Nakyanzi, *Smile, You're on Not-So-Candid Camera,* ABC News.com, *at* http://www.abcnews.go. com/sections/scitech/DailyNews/surveilcams010703.html (last visited Sept. 10, 2002) (discussing why Tampa's Ybor City was chosen to test system).

55. Kasindorf, *supra* note 4, at http://www.usatoday.com/life/cyber/tech/2001-08-02-big-brother-cameras.htm (describing city's use of face recognition technology and constitutionality of such technology).

56. *See id.* (reporting presence of cameras in Tampa); Nakyanzi, *supra* note 54, at http://www.abcnews.go.com/sections/scitech/DailyNews/surveilcams010703.html (describing use of cameras).

57. *See* Kasindorf, *supra* note 4, at http://www.usatoday.com/life/cyber/tech/2001-08-02-big-brother-cameras.htm (describing police monitoring); Nakyanzi, *supra* note 54, at http://www.abcnews.go.com/sections/scitech/ DailyNews/surveilcams010703.html (noting use of 30,000 photographs in database); *Proposal Wants to Keep Big Brother's Eye Shut,* Yahoo! News (Aug. 21, 2001), *at* http://dailynews.yahoo.com/htx/wjxt/20010821/lo/889412_1.html (discussing use of technology in Tampa).

58. *See* Anderson, *supra* note 4, at http://news.bbc.co.uk/hi/english/sci/tech/ newsid_1500000/1500017.stm (reporting on protests); Robert MacMillan, *Jacksonville Official Fights Face-Recognition Technology,* Newsbytes (Aug. 23, 2001), *at* http://www.newsbytes.com/news/01/169348.html (discussing unhappiness with use of technology); Mac McKerral, *Ybor City: Eye in the Sky, Catching Crooks on the Sly,* TAMPA BAY BUS. J., July 20, 2001 (mentioning residents' unhappiness with cameras being used to watch them); *Proposal Wants to Keep Big Brother's Eye Shut, supra* note 57, at http://dailynews.yahoo.com/htx/wjxt/ 20010821/lo/889412_1.html (reporting on citizens' dislike of technology). This July, about 100 people protested the use of the cameras. *See* Anderson, *supra* note 4, at http://news.bbc.co.uk/hi/english/ sci/tech/newsid_1500000/1500017.stm (reporting on protests). Some City Council members have also expressed their concern with the use of the cameras. *See id.* (expressing concern of City Council members).

caused the Tampa City Council to reconsider the use of the surveillance system.[59]

As a result of the technology's initial uses at the Super Bowl and in Tampa, other states are moving toward incorporating this new form of surveillance into their own standard procedures.[60] For example, Colorado passed a bill in mid-2001 requiring an individual to have his or her picture taken when applying for or renewing a driver's license.[61] The state will then compile the photos into a database of Colorado drivers to scan for individuals with outstanding warrants or criminal histories.[62] The state will also enter these photographs into a larger federal database that is

59. *See* Anderson, *supra* note 4, at http://news.bbc.co. uk/hi/english/sci/tech/newsid_1500000/1500017.stm (discussing Council's vote); Kinsler, *supra* note 36, at http://www.abatesc.com/news/news-6-aug-01.htm (reporting vote of City Council); Robert MacMillan, *Tampa Face-Recognition Vote Rattles Privacy Group—Update*, Newsbytes (Aug. 3, 2001), *at* http://www.newsbytes.com/news/01/168677.html (noting controversy in City Council over use of technology). Recently, two City Council members motioned to have the city terminate its contract for its use of the face recognition system. *See* Kinsler, *supra* note 36, at http://www.abatesc.com/news/news-6-aug-01.htm (discussing controversy in City Council). Although the decision to cancel the contract was left up to the sole discretion of Mayor Dick Greco, the City Council vote was a chance to gauge the response to recent questions regarding the privacy concerns arising from using this new technology. *See id.* (recognizing importance of vote). Nevertheless, the Council narrowly voted to maintain the system until it is demonstrated that the system does not work. *See id.* (reporting final vote).

60. *See* Blum, *supra* note 2, *at* http://www.pilotonline.com/news/nw0711nay.html (discussing Virginia's plan to implement new technology). Virginia is one state that is making plans to install face recognition technology in order to beef up security at its oceanfront. *See id.* (reporting Virginia's plan to install system). Currently, Virginia Beach's police department is in the process of constructing a presentation aimed at getting the city council to approve the implementation of the new technology. *See id.* (documenting Virginia's plan). Even though there has not yet been a formal proposal made, many city council members, as well as the mayor, have come out against the plan, claiming that "[i]t's definitely like Big Brother." *Id.* (reporting local government's reaction to plan). The police hope to compile a database filled with photographs of criminals, runaways and missing people. *See id.* (noting police's plan to create database to help capture criminals and missing people). The city may be the potential recipient of a $150,000 grant from the Virginia Department of Criminal Justice, which would leave only $50,000 that the city would have to contribute. *See id.* (discussing grant and costs to city in order to implement new technology).

61. *See* Julia C. Martinez, *Colo. to 'Map' Faces of Drivers*, DENVERPOST.COM (July 4, 2001), *available at* http://www.denverpost.com/Stories/0,1002,11%257E57823,00.html (noting "[o]ld driver's license photos will be scanned into a computer database . . . ."); Martinez, *supra* note 44, at http://www.denverpost.com/Stories/0,1002,53%257E70770,00.html (discussing new law); Editorial, *Now, High-Tech Mug Shots*, DENVER POST.COM (July 9, 2001), *available at* http://www.denverpost.com/Stories/0,1002,417%257E62231,00.html (discussing new license system).

62. *See* Martinez, *supra* note 61, at http://denverpost.com/ Stories/0,1002,11%257E57823,00.html (discussing law requiring picture for all who want driver's license); Martinez, *supra* note 44, at http://www.denverpost.com/Stories/0,1002, 53%257E70770,00.html (describing new law); *Now, High-Tech Mug Shots*, *supra* note 61, at http://www.denverpost.com/Stories/0,1002,417%257E62231,00.html (reporting on new plan for driver's license photographs).

currently under construction.[63] A backlash from the citizens of Colorado, however, has caused the state to reconsider its new policy.[64] Colorado's governor asked the state to postpone implementing the new program in order to examine the potential privacy abuses that might arise from the technology's use.[65]

The United States is not the only country utilizing face recognition systems.[66] In fact, England was one of the first nations to capitalize on this new technology.[67] Since the fall of 1998, Newham, England, a borough of London, began monitoring its citizens with the same face recognition system used at the Super Bowl.[68] Cameras monitor the area and try to match the images against a database of known criminals.[69] As a result, many credit the system with helping to reduce crime in the area by almost forty percent in the first year alone.[70] British officials were so impressed with

63. *See* Martinez, *supra* note 61, at http://denverpost.com/Stories/0,1002,11%257E57823,00.html (noting use of database); Martinez, *supra* note 44, at http:// www.denverpost.com/Stories/0,1002,53%257E70770,00.html (reporting on use of license photographs); *Now, High-Tech Mug Shots*, *supra* note 61, at http://www.denverpost.com/Stories/0,1002,417%257E62231,00.html (discussing use of photographs).

64. *See* Julia C. Martinez, *Approval of Facial Mapping Reviewed*, DENVER POST, July 15, 2001, at A8 (discussing review of new policy); *Owens' Balancing Act*, *supra* note 16, at A12 ("We're in favor of using face recognition to stop identity theft and catch crooks, but we don't want government using it to snoop on ordinary citizens.").

65. *See* Martinez, *supra* note 64, at A8 (noting "Owens said he's considering an executive order to place safeguards into the law to prevent use of the new technology to further invade citizens' privacy."); *Owens' Balancing Act*, *supra* note 16, at A12 (discussing Governor Owens's call to revisit new policy). Many of the state lawmakers have acknowledged that when they were voting to approve the new policy, they were not aware that they were actually voting to install face recognition technology. *See* Martinez, *supra* note 64, at A8 (noting confusion over policy).

66. For a further discussion of other countries that have instituted this new technology, see *infra* notes 152-53.

67. *See Face Recognition Technology—Big Brother Arrives*, *supra* note 17, at A15 (noting "high-tech surveillance by the [British] government is much more accepted than in the United States"); Julia Scheeres, *Some Camera to Watch over You*, WIRED NEWS (Apr. 5, 2001), *at* http://www.wired.com/news/print/0,1294,42794,00.html (last visited Sept. 17, 2002) (noting Britain is "the world leader in video surveillance use").

68. *See Face Recognition Technology is Next—Big Brother Arrives*, *supra* note 17, at A15 (discussing use of system in England); Kasindorf, *supra* note 4, at A3 (noting cameras have been responsible for less than ten arrests); Ellis, *supra* note 3, at http://www.wired.com/news/print/0,1294,38775,00.html (noting system's presence in Newham, England).

69. *See Face Recognition Technology is Next—Big Brother Arrives*, *supra* note 17, at A15 (discussing England's use of face recognition technology); Ellis, *supra* note 3, at http://www.wired.com/news/print/0,1294,38775,00.html (noting over 200 cameras search for known criminals on Newham's streets); Scheeres, *supra* note 67, at http://www.wired.com/news/print/0,1294,42794,00.html (noting in England "the unblinking eyes of security cameras are as much a part of the landscape as Big Ben").

70. *See* Anderson, *supra* note 4, at http://news.bbc.co. uk/hi/english/sci/tech/newsid_1500000/1500017.stm (finding forty percent drop in crime); Ellis,

the new technology that they announced a plan in 2000 to expand its use.[71] They expected to install almost two million cameras across the country to aid law enforcement officials.[72]

III. HISTORY OF PRIVACY IN PUBLIC PLACES

Although the United States Supreme Court has never directly addressed the issue of face recognition technology, the Court has decided a number of other cases that provide guidance for analyzing the legality of this new technology.[73] Since the mid-1960s, the Supreme Court has addressed issues concerning privacy rights under the Fourth Amendment and self-incrimination under the Fifth Amendment.[74] By examining the Court's history in addressing and analyzing these issues, it is possible to develop a legal framework in which to analyze the legality of face recognition technology.[75]

---

supra note 3, at http://www.wired.com/news/print/ 0,1294,38775,00.html (observing decrease in criminal activity); *Face Recognition Technology is Next—Big Brother Arrives, supra* note 17, at A15 (noting "Newham officials say the system has significantly reduced crime"); Scheeres, *supra* note 67, at http://www. wired.com/news/print/0,1294,42794,00.html (discussing beneficial effects of technology in England). Face recognition technology and surveillance in general have been in wide use throughout England. *See id.* ("The British government is so enthralled with the technology that it announced plans to increase the number of cameras in England . . . .").

71. *See Face Recognition Technology is Next—Big Brother Arrives, supra* note 17, at A15 (describing plans in Britain to expand use of surveillance cameras).

72. *See id.* (describing plans to expand camera usage).

73. For a further discussion of court cases providing a framework for the legal analysis of face recognition technology, see *infra* notes 74-109 and accompanying text.

74. *See generally* Kyllo v. United States, 533 U.S. 27 (2001) (addressing issues regarding use of thermal imaging); Doe v. United States, 487 U.S. 201 (1988) (discussing self-incrimination privilege); Cal. v. Ciraolo, 476 U.S. 207 (1986) (determining constitutionality of arial observation when it is not of defendant's property and is done without warrant); Smith v. Md., 442 U.S. 735 (1979) (discussing constitutionality of pen register); Fisher v. United States, 425 U.S. 391 (1976) (discussing self-incrimination privilege); United States v. Dionisio, 410 U.S. 1 (1973) (discussing constitutionality of disclosing voice exemplars in front of grand jury); Gilbert v. Cal., 388 U.S. 263 (1967) (discussing defendant's right to have counsel present when presented in line-up); Katz v. United States, 389 U.S. 347 (1967) (finding expectation of privacy when using phone booth); United States v. Wade, 388 U.S. 218 (1967) (discussing defendant's right to have counsel present when placed in line-up); Schmerber v. Cal., 384 U.S. 757 (1966) (discussing constitutionality of blood test performed in order to determine whether defendant was driving while intoxicated); Breithaupt v. Abram, 352 U.S. 432 (1957) (same).

75. For a complete analysis of the legality of face recognition technology, see *infra* notes 110-47 and accompanying text.

A. *Privacy and the Fourth Amendment*

The most important decision from the Court regarding privacy under the Fourth Amendment was the 1967 decision of *Katz v. United States*.[76] In *Katz*, the Court acknowledged that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[77] The Court held, however, that the Fourth Amendment was designed to protect individual privacy against certain kinds of governmental intrusion.[78] Most importantly, *Katz* established a two-pronged test to determine whether the Fourth Amendment protects an activity from governmental intrusion: 1) whether there is an actual expectation of privacy; and 2) whether that expectation is one which society is willing to recognize as reasonable.[79] Since *Katz*, the Court has consistently upheld the notion that no reasonable expectation of privacy exists for things that a person exposes to the public.[80] This notion is increasingly important when considering the dra-

76. 389 U.S. 347 (1967). This case came before the Supreme Court after the defendant was convicted of placing a wager over the telephone from Los Angeles to Miami and Boston. *See id.* at 348 (detailing facts of case). These wagers were placed from a telephone booth and FBI agents used an electronic listening device to record the petitioner's conversations. *See id.* at 348-49 (explaining events leading up to case). The petitioner contended that these conversations were recorded in violation of the Fourth Amendment, however the court of appeals disagreed. *See id.* (noting lower court's decision). The Supreme Court heard the case to decide whether a public phone booth was a constitutionally protected area and whether a physical invasion into a constitutionally protected area was required in order to violate the Fourth Amendment. *See id.* at 353-54 (listing issues of case).

77. *See id.* at 350 (discussing that Fourth Amendment protections go further than privacy and "often have nothing to do with privacy at all"). The Court noted that personal privacy is protected from government intrusion by a number of provisions in the Constitution. *See id.* at 350-51 (analyzing purpose of Fourth Amendment). Despite the protections offered by the Constitution, "the protection of a person's *general* right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual States." *Id.*

78. *See id.* at 350 (recognizing protections provided by Fourth Amendment). The Fourth Amendment states "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV.

79. *See Katz*, 389 U.S. at 360-61 (Harlan, J., concurring) (describing two-pronged test).

80. *See, e.g.*, Cal. v. Ciraolo, 476 U.S. 207, 215 (1986) (delineating holding of case); Smith v. Md., 442 U.S. 735, 742-44 (1979) (same). In *Smith*, the Court addressed the issue of whether the use of a pen register by police amounted to a Fourth Amendment search. *See id.* at 736 (noting issue of case). The police suspected Smith in a robbery and had the telephone company place a pen register on his telephone to record the numbers he dialed from his home. *See id.* at 737 (discussing facts surrounding case). Although the police did not obtain a warrant for the pen register, the information they obtained from it was later used to obtain a warrant for Smith's home. *See id.* (describing evidence in question). Smith was later arrested and at his trial, he sought to exclude all evidence obtained from the use of the pen register under the theory that its use constituted a search without a warrant, thereby violating the Fourth Amendment. *See id.* (outlining defendant's argument). The Court rejected this argument, holding that individuals have no

matic technological innovations that allow the government to use an individual's personal characteristics to identify him or her.[81]

One of the main cases addressing the use of personal characteristics, and closely related to the issue of face recognition technology, is *United States v. Dionisio*.[82] The issue in *Dionisio* was whether an individual's voice

---

reasonable expectation of privacy in the telephone numbers they dial. *See id.* at 742 (holding no privacy in telephone numbers dialed). In its holding, the Court acknowledged that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44.

In *Ciraolo*, the Court addressed the idea of whether the warrantless aerial viewing of an individual's fenced-in backyard constitutes an unreasonable search under the Fourth Amendment. *See Ciraolo*, 476 U.S. at 209 (noting issue in case). In this case, the police had received an anonymous tip that Ciraolo was growing marijuana in his backyard. *See id.* (detailing facts of case). The police were unable to see over the fence surrounding the yard, so they used a private plane to fly over Ciraolo's home and backyard. *See id.* (outlining method used to detect marijuana). During the flight, the police were able to identify marijuana, which they photographed using a standard camera. *See id.* (describing how drugs were discovered). A warrant was subsequently issued, the marijuana plants were seized and Ciraolo was arrested. *See id.* at 209-10 (discussing facts of case). At trial, Ciraolo moved to have the evidence excluded, claiming that it was obtained subsequent to a warrantless search of his backyard violating the Fourth Amendment. *See id.* at 210 (noting defendant's argument). The Court, on appeal, did not agree with this reasoning and held that an aerial search of an individual's backyard was not a Fourth Amendment search. *See id.* at 215 (holding Fourth Amendment was not violated). Again, the Court upheld the idea that the Fourth Amendment does not protect that which is "visible to the naked eye." *Id.* at 215.

81. For a further discussion of the impact of the decision in *Katz* on technological innovations used by the government to observe individuals, see *infra* notes 114-26 and accompanying text.

82. 410 U.S. 1 (1973). The Court heard this case in order to decide whether the use of voice exemplars was a search under the Fourth Amendment. *See id.* at 3 (noting issue in case). In this case, a grand jury was convened to investigate a possible violation of federal gambling laws. *See id.* at 2 (reciting facts of case). During the grand jury investigation, a number of voice recordings were entered into evidence. *See id.* (discussing evidence in question). To identify the voices on the recordings, the grand jury issued subpoenas to approximately twenty individuals, to obtain voice exemplars. *See id.* at 3 (describing method by which evidence was gathered). Each individual was requested to read a sample of the conversation already entered into evidence and this reading was then recorded. *See id.* (noting request for voice samples). These voice samples were then compared with the recording already in evidence, in order to discover a match. *See id.* (setting forth role evidence would play in case). Dionisio refused to furnish the grand jury with the voice sample, claiming it violated his rights under the Fourth Amendment. *See id.* (explaining defendant's argument over evidence's constitutionality).

In *Dionisio*, the defendant also raised the issue of the Fifth Amendment privilege against self-incrimination. *See id.* at 5 (noting issue raised in case). The Court held that it was a long-standing principle that "the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against compulsory self-incrimination." *Id.* at 5-6. For a complete discussion of the Fifth Amendment privilege against self-incrimination, see *infra* notes 94-109 and accompanying text.

could be used to identify him.[83] The Court held that because the Fourth Amendment does not protect what "'a person knowingly exposes to the public,'" there is no right to privacy in an individual's voice.[84]

The Court in *Dionisio* also acknowledged that an individual has no reasonable expectation of privacy in his own face, as it is constantly exposed to the public.[85] In *Davis v. Mississippi*,[86] the Court expanded this idea by noting that fingerprinting also does not constitute an invasion of privacy because it "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[87] The Court reasoned that because fingerprinting, like voice identification, does not require any intrusiveness or penetration "beyond the body's surface," it does not implicate the dignity or privacy of an individual at a level that would give rise to Fourth Amendment protection.[88] These cases solidify the Court's jurisprudence that forms of surveillance or identification that rely on an individual's characteristics that are constantly exposed to the public including one's voice, fingerprints and facial characteristics, are not protected under the Fourth Amendment.[89]

The last word from the Supreme Court on the issue of privacy was in 2001.[90] According to the Court in *Kyllo v. United States*,[91] the use of a thermal imaging device to scan a home was considered a search and, absent a valid search warrant, violated the Fourth Amendment.[92] Despite

83. *See Dionisio*, 410 U.S. at 3 (summarizing facts of case). For a complete discussion of the facts of *Dionisio*, see *supra* note 82.

84. *See id.* at 14 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

85. *See Dionisio*, 410 U.S. at 14 ("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.").

86. 394 U.S. 721 (1969).

87. *Id.* at 727.

88. *See id.* (setting limits of Fourth Amendment protection, as well as what constitutes Fourth Amendment search).

89. *See generally Dionisio*, 410 U.S. at 1 (defining limits of Fourth Amendment protection); *see also generally* Cal. v. Ciraolo, 476 U.S. 207 (1986) (same); Smith v. Md., 442 U.S. 735 (1979) (same); *Davis*, 394 U.S. at 721 (same); Katz v. United States, 386 U.S. 347 (1967) (same).

90. *See generally* Kyllo v. United States, 533 U.S. 27, 31 (2001) (analyzing Fourth Amendment issues related to use of thermal imaging device).

91. 533 U.S. 27 (2001).

92. *See id.* at 34 ("To withdraw protection of this minimum [privacy] expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."). In 1991, petitioner was suspected of growing marijuana in his home. *See id.* at 29-30 (outlining facts giving rise to case). To grow marijuana inside the home, an individual needs high power lamps. *See id.* (noting technology required to grow marijuana). To detect the presence of these lamps, two agents from the Department of the Interior used thermal imaging devices to scan Kyllo's home and the other homes in his complex. *See id.* (detailing method used by police to search individual's home). The imaging devices are designed to detect infrared radiation, emitted by almost all objects, but not visible to the naked eye. *See id.* (summarizing method used by thermal imagers). The imagers are also able to indicate the heat generated by the objects by dividing the radiation emitted into

the limits this holding seems to place on the use of forms of electronic surveillance, *Kyllo* only protects individuals when they are inside their homes, and offers citizens no protection when they are in public, thereby retaining the notion that individual privacy is unprotected when an individual willingly exposes something to the public.[93]

B. *Self-incrimination and the Fifth Amendment*

The Supreme Court established the parameters of the Fifth Amendment privilege against self-incrimination in the 1966 decision of *Schmerber v. California*.[94] In *Schmerber*, the Court limited the Fifth Amendment protections to certain types of information.[95] The Court held that the Fifth

---

categories: black is cool, white is hot and gray falls somewhere between the two. *See id.* (noting capabilities of imagers). The scan of the homes was conducted by the agents in a car across from the house and revealed that certain parts of the Kyllo's house were significantly hotter when compared to other parts of the house and the other houses in the complex. *See id.* (summarizing facts of case). Using this information, combined with informant tips and Kyllo's utility bills, a search warrant was issued for Kyllo's home. *See id.* (discussing how warrant was obtained). The search revealed that Kyllo was in fact using high-powered halide light to grow marijuana inside and he was subsequently arrested. *See id.* (detailing results of search). Kyllo sought to suppress the evidence on the theory that the use of the thermal imager was an unconstitutional search under the Fourth Amendment. *See id.* (outlining defendant's argument).

93. *See id.* at 34 (applying *Katz* test). "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' . . . constitutes a search—at least where (as here) the technology in question is not in general public use." *Id.*

94. 384 U.S. 757 (1966). The Court heard this case in order to determine whether an individual who had a blood sample taken for a blood alcohol test was forced to be a witness against himself, violating the Fifth Amendment. *See id.* at 759 (questioning legality of blood alcohol test). Schmerber had been in a car accident and was taken to the hospital for the treatment of his injuries. *See id.* at 758 (outlining facts in case). While at the hospital, Schmerber was arrested by police for driving under the influence. *See id.* (describing events leading up to case). At the hospital, police directed a doctor to draw a sample of blood from Schmerber. *See id.* (examining method by which sample was obtained). Tests on the blood sample indicated that Schmerber's blood alcohol level was over the legal limit at the time of the accident. *See id.* at 759 (discussing results of blood test). Schmerber's blood alcohol level was entered into evidence at his trial. *See id.* (outlining use of blood alcohol level at trial). He objected to its admittance, claiming that the blood sample was drawn despite his refusal and it amounted to a violation of his Fifth Amendment privilege against self-incrimination. *See id.* (noting defendant's objections). The Court did not support this reasoning, holding that the evidence did not fall into the scope of evidence protected under the Fifth Amendment. *See id.* at 764 (analyzing scope of Fifth Amendment).

95. *See id.* ("[Fifth Amendment] offers no protection against compulsion to submit to fingerprinting, photographing . . . ."). The Court held, more specifically, that "the privilege [against self-incrimination] is a bar against compelling 'communications' or 'testimony,' but that compulsion which makes a suspect or accused the source of 'real or physical evidence' does not violate it." *Id.*

In this statement, the Court held that where the individual himself is the evidence, either in his face, features or even his own blood, the use of that informa-

Amendment protects an individual from being forced to provide the government with "evidence of a testimonial or communicative nature."[96] The Court stated that fingerprints, photographs, voice and stance are not protected as evidence that is testimonial or communicative in nature.[97] Furthermore, the Court has consistently held that compelling evidence including a blood test, which goes beyond the body's surface, is not considered testimonial or communicative and is not protected by the Fifth Amendment.[98]

In *Gilbert v. State of California*,[99] the Court stretched this reasoning to cover an individual's handwriting in holding that "[a] mere handwriting exemplar, in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic outside [the Fifth Amendment's] protection."[100] The Court again extended this reasoning

---

tion as evidence does not rise to the level of being testimonial or communicative in nature and is therefore not protected under the Fifth Amendment. *See id.* at 761-64 (discussing limits of Fifth Amendment).

96. *See id.* at 761. The Fifth Amendment states that no "person be compelled, in any criminal case, to be a witness against himself, nor be deprived of life, liberty or property, without due process of law." U.S. CONST. amend. V. In *Schmerber*, the Court examined the policies surrounding the Fifth Amendment and firmly established the parameters of what evidence it protects. *See Schmerber*, 384 U.S. at 762 (analyzing purpose of Fifth Amendment).

> All these policies point to one overriding thought: the constitutional foundation underlying the privilege is the respect a government—state or federal—must accord to the dignity and integrity of its citizens. To maintain a "fair state-individual balance," to require the government "to shoulder the entire load," . . . to respect the inviolability of the human personality, our accusatory system of criminal justice demands that the government seeking to punish an individual produce the evidence against him by its own independent labors, rather than by the cruel, simple expedient of compelling it from his own mouth.

Id. (citing Miranda v. Ariz., 384 U.S. 436, 460 (1966)). The Court acknowledged that "[i]t is clear that the protection of the privilege reaches an accused's communications, whatever form they might take, and the compulsion of responses which are also communications . . . ." *Schmerber*, 384 U.S. at 763-64. In this case, however, the drawing of Schmerber's blood did not amount to a communication and was not protected under the Fifth Amendment. *See id.* at 761 (holding blood test did not violate Fifth Amendment).

97. *See id.* at 764 (holding Fifth Amendment offers no protection against compulsion to submit to "fingerprinting, photographing, or measurements, to write or speak for identification").

98. *See generally id.* (defining limits of Fifth Amendment protection); *see also generally* Gilbert v. Cal., 388 U.S. 263, 266-67 (1967) (same); Breithaupt v. Abram, 352 U.S. 432, 439-40 (1957) (same).

99. 388 U.S. 263 (1967).

100. *See id.* at 266-67. In its holding, the Court acknowledged that an individual's handwriting is in fact a means of communication, however not every communication is protected by the Fifth Amendment. *See id.* at 266 (setting limits on Fifth Amendment protection). The Court noted that the content of handwritten communications can rise to the level of a communication that is protected under the Fifth Amendment, however handwriting itself offered no such protection. *See id.* at 267 (finding that handwriting is not protected because it is "an identifying physical characteristic").

in *United States v. Wade*,[101] when it held that compelling an individual to submit to a lineup does not amount to self-incrimination and is not protected by the Fifth Amendment.[102] In *Wade*, the Court reasoned that because the accused is merely required to show his face and not required to divulge any information he might possess in a line-up, there is no protection under the Fifth Amendment.[103]

In 1988, the Court solidified its jurisprudence regarding the Fifth Amendment in *Doe v. United States*,[104] when it held that "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[105] Once again, the Court upheld the notion that the privilege against self-incrimination only comes into play when the government compels an individual to give some kind of testimonial communication.[106]

Despite the fact that the legality of face recognition technology remains untested in the court system, the history of Supreme Court decisions regarding privacy and self-incrimination, makes it possible to examine how the Court would react to Constitutional challenges to this new technology.[107] Applying the rules that the Court has laid out in its previous cases, it is clear that the Fourth and Fifth Amendments protect *governmental* use of face recognition technology.[108] In the hands of private

101. 388 U.S. 218 (1967).

102. *See id.* at 222 (holding that forcing individual to take part in lineup does not involve compulsion to give evidence that is testimonial in nature).

103. *See id.* (noting lineup involves "compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge").

104. 487 U.S. 201 (1988). John Doe was the suspect of "possible federal offenses arising from suspected fraudulent manipulation of oil cargoes and receipt of unreported income." *Id.* at 202. Doe had to appear before a grand jury and they subpoenaed records of his bank accounts. *See id.* (discussing facts of case). While Doe produced some of the requested documents, he denied the possession of others, citing his Fifth Amendment privilege against self-incrimination. *See id.* at 202-03 (outlining defendant's argument). The grand jury also subpoenaed the records of three foreign banks with whom Doe did business. *See id.* at 203 (noting initial inability to obtain documents). The banks refused to turn the records over, citing their privacy policies, which do not allow them to turn over records without the customer's consent. *See id.* (discussing privacy policies of banks). The government subsequently filed a motion with the district court, asking for a court order forcing Doe to sign consent forms to allow the banks to turn over his records. *See id.* (summarizing facts of case). The court refused to grant the motion and the case eventually came before the Supreme Court to decide whether a court order forcing an individual to authorize his bank to turn over financial statements violated the Fifth Amendment privilege against self-incrimination. *See id.* at 206 (examining lower court decision).

105. *Id.* at 210.

106. *See id.* (citing Schmerber v. United States, 384 U.S. 757, 761 (1966) (defining boundaries of privilege against self-incrimination)).

107. For a further discussion of the legality of face recognition technology, see *infra* notes 110-47 and accompanying text.

108. For a further discussion of the legality of face recognition technology in the hands of the government, see *infra* notes 113-37 and accompanying text.

citizens, however, the use of this technology continues to raise a number of questions.[109]

IV. PRIVACY IMPLICATIONS OF FACIAL RECOGNITION TECHNOLOGY

The events at the 2001 Super Bowl, coupled with the fact that this new technology and the legal issues raised remain untested in a courtroom, have lead to an onslaught of individuals questioning the privacy implications that arise from the use of face recognition software.[110] This technology is used in two main areas: by the government and by private individuals.[111] For government use of face recognition, the applicable limitations are located in the Fourth and Fifth Amendments.[112]

---

109. For a further discussion of the legality of the use of face recognition technology in the hands of third parties, see *infra* notes 138-47 and accompanying text.

110. *See generally* JOHN D. WOODWARD, JR., SUPER BOWL SURVEILLANCE: FACING UP TO BIOMETRICS 7-8 (Rand Arroyo Center May 2001) (discussing issues raised by face recognition technology); Kathryn Balint, *Who Are You? Technology Plays Key Role in New Efforts to Verify Identity*, SAN DIEGO UNION-TRIB., Sept. 25, 2001, at Computer Link 6; Grayson Barber, *Public Video Surveillance Erodes Our Integrity*, 165 N.J. L.J. 427 (same); Barbara Rose, *High-Tech Security on Stage; Events of Sept. 11 Put ID Devices in the Spotlight*, CHI. TRIB., Sept. 24, 2001, at Business 1 (same); Harvey A. Silverglate, *Who Gets to Do the Taping?*, NAT'L L.J., Aug. 20, 2001, at A25 (same); *Digital Big Brother*, *supra* note 4, at C18 (same); *CNN Live This Morning: America's New War: Look at Some Security Measures that Could be Put into Place* (CNN television broadcast, Oct. 1, 2001) (transcript on file with author) (same); *Today: Security Cameras on the Rise; Charles Shoebridge, Scotland Yard, Comments on Camera—Film Evidence to Catch Criminals; Privacy Concerns of Other Surveillance Systems* (NBC television broadcast, Sept. 27, 2001) (transcript on file with author) (same); *Biometrics and Privacy: Industry Policy on Crowd Surveillance*, Int'l Biometric Indus. Ass'n (Feb. 2, 2001), *available at* http://www.ibia.org/pressrelease19.htm (last visited Aug. 16, 2001) (same); Heather Green, *Technology's Creeping Threats to Privacy*, BUS. WK. ONLINE (Aug. 13, 2001), *at* http://www.businessweek.com/technology/content/aug2001/tc20010813_691.htm (last visited Aug. 16, 2001) (same); Thomas C. Greene, *Think Tank Urges Face-Scanning of the Masses*, Register (Aug. 13, 2001), *at* http://www.theregister.co.uk/content/6/20966.html (last visited Sept. 3, 2002) (same); Nuger, *supra* note 5, at http://www.engr.sjsu.edu/biometrics/publications_consideration.html (same); Paul O'Shea, *Watching the Watchers*, ChipCenter *at* http://www.chipcenter.com/analog/ed002.htm?PRINT=true (last visited Sept. 3, 2002) (same); Andy Sullivan, *Security Firms Call for Video-Surveillance Law*, Yahoo! News (Aug. 8, 2001), *at* http://dailynews.yahoo.com/h/nm/20010808/tc/tech_privacy_surveillance_dc_1.html (last visited Sept. 4, 2002) (same); Dr. George Tomko, *Biometrics as a Privacy-enhancing Technology: Friend or Foe of Privacy?*, Privacy Laws & Bus. 9th Privacy Commissioners'/Data Protection Authorities Workshop (Sept. 15, 1998), *available at* http://www.dss.state.ct.us/digital/tomko.htm (last visited Sept. 7, 2002) (same).

111. For a further discussion of the government's use of face recognition technology, see *infra* notes 113-37 and accompanying text. For a further discussion of private individual's use of face recognition technology, see *infra* notes 138-47 and accompanying text.

112. *See* Barber, *supra* note 2, at http://www.chipcenter. com/columns/COL_20010718.html ("Cast strictly in terms of constitutional law, the legal case against video surveillance and face recognition technology rests on the Fourth and Fifth Amendments, which protect against unreasonable searches and seizures and

A. *Governmental Use of Biometrics*

1. *The Fourth Amendment*

One of the main concerns with face recognition technology is that using surveillance cameras amounts to a search and is therefore subject to the restraints of the Fourth Amendment.[113] The Supreme Court has held that the Fourth Amendment applies to people and not to places.[114] More specifically, to determine whether government use of face recognition technology violates the Fourth Amendment, courts should apply the *Katz* two-prong test.[115] The first question is whether an individual has an actual expectation of privacy.[116] In considering this issue, it should be emphasized that the Court has consistently held that an individual has no valid expectation of privacy in something he or she willingly exposes to the public.[117] By choosing to walk the streets, attend a sporting event or go to the store, an individual is choosing to expose his or her likeness to the public and anything he or she may encounter on the streets, including surveillance cameras.[118] The Court has acknowledged that

---

self-incrimination."); Nuger, *supra* note 5, at http://www. engr.sjsu.edu/biometrics/publications_consideration.html (analyzing face recognition technology in terms of Fourth and Fifth Amendments); O'Shea, *supra* note 110, at http://www.chipcenter.com/analog/ed002.htm (noting Fourth and Fifth Amendments form basis of analysis of face recognition technology).

113. *See* McCullagh, *supra* note 46, at http://www.wired. com/news/print/0,1294,41571,00.html (quoting American Civil Liberties Union concern that face recognition technology "raises serious concerns about the Fourth Amendment right of all citizens to be free of unreasonable searches and seizures").

114. *See* William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1266 (1999) (noting "[p]rivacy, in Fourth Amendment terms, is something that exists only in certain types of spaces").

115. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (establishing two-prong test for Fourth Amendment protection). In *Katz*, Justice Harlan articulated the two-pronged test that applies in cases concerning an invasion of Fourth Amendment privacy. *See id.* (setting forth test). "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.*

116. *See id.* (discussing prongs of test). In *Katz*, the issue was whether an individual has an actual expectation of privacy in his or her personal characteristics when he or she is walking down the street or is present inside a store or business. *See id.* at 361-62 (clarifying two-pronged test applicable to Fourth Amendment issues).

117. *See id.* at 353 (holding that government action of listening to conversation in phone booth violated Fourth Amendment); *see also* Cal. v. Ciraolo, 476 U.S. 207, 215 (1986) (deciding that police observation of yard from airplane does not violate Fourth Amendment); Smith v. Md., 442 U.S. 735, 745 (1979) (holding that Fourth Amendment not violated when police use pen register to record phone number dialed); Davis v. Miss., 394 U.S. 721, 727 (1969) (finding that fingerprinting does not violate Fourth Amendment).

118. *See Digital Big Brother*, *supra* note 4, at C18 ("According to law, a person has no expectation of privacy when he or she chooses to be in a public place."); McCullagh, *supra* note 46, at http://www.wired.com/news/print/0,1294,41571,00.

> [t]he physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. *Like a man's facial characteristics*, or handwriting, his voice is repeatedly produced for others to hear. 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.*[119]

Because an individual regularly exposes his or her face to the world, there is no Fourth Amendment violation when that face is photographed.[120]

Even if a court would find that individuals do possess actual expectations of privacy when they are out in public, *Katz* also requires that the expectation be one that society is willing to recognize as being reasonable.[121] This determination involves balancing society's desire to protect the public safety against individual privacy. The increasing desire to protect public safety, however, would likely overshadow any personal privacy interest that individuals may have when they are in public.[122] Most Americans are not, and may never be, ready to accept that an individual can expect to maintain his or her privacy when he or she is in public. Without society's willingness to protect an individual's privacy in his or her counte-

---

html ("'There's no Fourth Amendment problem if the government is simply observing—or even recording what goes on in public . . . .'"); O'Shea, *supra* note 110, at http://www.chipcenter.com/analog/ed002.htm ("[A] person does not have a reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public . . . .").

119. United States v. Dionisio, 410 U.S. 1, 14 (1973) (emphasis added). The Court did uphold a narrow exception to this rule, as offered by the Court of Appeals for the Second Circuit:

> Except for the rare recluse who chooses to live his life in complete solitude, in our daily lives we constantly speak and write, and while the content of a communication is entitled to Fourth Amendment protection . . . the underlying identifying characteristics—the constant factor throughout both public and private communications—are open for all to see or hear.

Id. In upholding the Second Circuit's statement, the Supreme Court held that while characteristics an individual regularly exposes to the public are not protected under the Fourth Amendment, there is a small exception for individuals who have chosen to live their lives without public contact.

See id. (establishing small exception to rule that facial characteristics are not protected under Fifth Amendment).

120. *See* McCullagh, *supra* note 46, at http://www. wired.com/news/print/0,1294,41571,00.html (observing "there's no legitimate expectation of privacy"); O'Shea, *supra* note 110, at http://www.chipcenter.com/ analog/ed002.htm ("[L]aw enforcement's use of the technique at the Super Bowl does not appear to run afoul of the protections afforded by the U.S. Constitution.").

121. *See Katz*, 389 U.S. at 361 (1967) (laying out requirements of test). The second prong of the *Katz* test involves examining the reasonableness of an expectation that an individual can maintain his or her privacy while in public. *See id.* (articulating reasonableness prong of test).

122. *See id.* (noting requirements of second prong of test).

nance when he or she is in public, it cannot be protected by the Fourth Amendment.[123]

Because face recognition technology does not meet the test established by the Court in *Katz*, it is not a search under the Fourth Amendment.[124] If the use of face recognition systems are not considered searches, the government can use the technology in public places without violating individual privacy rights.[125] Although it appears that the use of face recognition technology would likely be protected under the Fourth Amendment, we cannot be sure of the outcome until the issue is resolved by a court.[126] As technology continues to advance, courts are forced to address the problems that arise from these new advances.[127] The Supreme Court's recent decision in *Kyllo v. United States*[128] recognized the Court's willingness to make room in the law for technological innovations.[129] The decision in *Kyllo*, however, is also important because it recognizes the Court's willingness to limit the use of certain types of electronic surveillance devices.[130] While the Court did limit its holding to the privacy of the home, *Kyllo* presents the possibility that in the future the Court could extend this privacy protection to public places.[131]

2. *The Fifth Amendment*

Another concern with face recognition technology is that by using an individual's face to identify him or her, an individual is forced to be a

123. *See* Fiona Harvey, *Technology that Stands Out from the Crowd: Biometric Security Systems*, FIN. TIMES (LONDON), Sept. 25, 2001, at 14 (discussing heightened need for security); Rose, *supra* note 110, at Business 1 (reporting on "a nation that increasingly will turn for protection to high-tech devices").

124. *See Katz*, 389 U.S. at 361 (laying out test). If an event or action does not meet the two prongs of the test set forth by Justice Harlan, it is not protected by the Fourth Amendment. *See id.* (noting certain events that do not meet test and are not protected by Fourth Amendment).

125. *See* WOODWARD, *supra* note 110, at 7 (analyzing technology in terms of Fourth Amendment).

126. *See* O'Shea, *supra* note 110, at http://www.chipcenter.com/ analog/ ed002.htm ("[L]aw enforcement's use . . . does not appear to run afoul of the protections afforded by the U.S. Constitution.").

127. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (deciding issue regarding use of thermal imaging device).

128. 533 U.S. 27 (2001).

129. *See id.* at 33-34 (addressing use of thermal imager).

130. *See id.* (limiting police use of thermal imagers). In its decision, the Court addressed the fact that changes in technology have an effect on an individual's privacy rights. *See id.* (addressing effect of technology). The Court noted "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Id.* The Court further recognized "[t]he question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id.*

131. *See id.* (leaving open issue of use of technology in public).

witness against him or herself, thereby violating the Fifth Amendment.[132] This is an issue the Court has addressed a number of times, continually holding that an individual's personal characteristics do not fall within the types of communications that are protected under the Fifth Amendment.[133] The Court has held that only evidence that is "testimonial or communicative in nature" falls within the umbrella of protection offered by the Fifth Amendment.[134] An individual's face is simply an identifying physical characteristic and is not considered a piece of evidence that contains any type of testimony or communication.[135] Just as an individual's forced participation in a line-up is not considered testimonial or communicative, it should follow that a photograph taken of an individual who is willingly in public is also not testimonial or communicative in nature.[136] Thus, individuals should not be considered witnesses against themselves when their photographs are taken as part of a face recognition system.[137]

B. *Third-Party Use of Biometrics*

The true privacy problems arise from third-party use of face recognition technology.[138] The biggest concern stemming from third party use is

132. *See* Barber, *supra* note 2, at http://www.chipcenter. com/clumns/COL_20010718.html ("Cast strictly in terms of constitutional law, the legal case against video surveillance and face recognition technology rests on the Fourth and Fifth Amendment . . . ."); Nuger, *supra* note 5, at http://www.engr.sjsu.edu/biometrics/ publications_consideration.html (analyzing face recognition technology in terms of Fifth Amendment); O'Shea, *supra* note 110, at http://www.chipcenter.com/analog/ed002.htm (noting Fifth Amendment serves as one basis for analysis of face recognition technology).

133. *See* Doe v. United States, 487 U.S. 201, 219 (1988) (holding that compelling individual to turn over bank records does not violate Fifth Amendment); Gilbert v. Cal., 388 U.S. 263, 266 (1967) (deciding that requiring handwriting samples does not violate Fifth Amendment); United States v. Wade, 388 U.S. 218, 221 (1967) (holding that requiring individual to take part in line-up does not violate Fifth Amendment); Schmerber v. Cal., 384 U.S. 757, 771 (1966) (finding that Fifth Amendment was not violated when suspect's blood was drawn).

134. *See Schmerber*, 384 U.S. at 761 (establishing parameters of Fifth Amendment protections).

135. *See Gilbert*, 388 U.S. at 266-67 (examining what means of communication are protected by Fifth Amendment). Because an individual's face does not in itself contain any type of testimony or communication, it is not considered the type of evidence that is protected by the Fifth Amendment. *See id.* at 266 ("The [Fifth Amendment] privilege reaches only compulsion of 'an accused's communications' . . . .").

136. *See Wade*, 388 U.S. at 222 ("We have no doubt that compelling the accused merely to exhibit his person for observation . . . involves no compulsion of the accused to give evidence having testimonial significance.").

137. *See id.* (holding there is no violation of Fifth Amendment when individual is required to show his or her face).

138. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com/introduction.html (discussing privacy concerns of biometric technology). "[T]he threat to privacy arises not from the positive identification that biometrics provide, but the ability of third parties to access this in identifiable form and link it to other information, resulting in secondary uses of that information without the consent

the potential for private citizens to develop and maintain vast amounts of information on individuals.[139] With the new technology being made available to the public, there is the possibility that businesses across the country will install surveillance cameras to scan the faces of their customers and employees.[140] There is also a fear that businesses will begin to develop data files on their customers and employees, and then share these files with other businesses.[141] The result is that businesses could track customer purchases or the whereabouts of their employees and every time individuals enter a store, their faces can call up their entire data file.[142]

Personal information is meant to remain private. Thus, the fact that technology is giving private individuals the power to recall personal information with a simple photograph raises concerns over the need to regulate this new technology.[143] While the Constitution may place limits on the government's use of this technology, there is no equivalent that regulates its use by private citizens.[144] Currently, there are no state or federal

---

of the data subject." *Id.*; *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 3 (2000) (commenting on erosion of privacy in America). Rosen comments that "the erosion of privacy, at home, at work, and in cyberspace, so that intimate personal information—from diaries, e-mail, and computer files to records of the books we read and the Web sites we browse—is increasingly vulnerable to being wrenched out of control and exposed to the world." *Id.*

139. *See* Green, *supra* note 110, at http://www.business week.com/technology/content/aug2001/tc20010813_691.htm (questioning "[w]hat's to stop commercial companies from acquiring these public records and selling them").

140. *See* Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.htm (discussing dangers of biometrics).

141. *See* WOODWARD, *supra* note 110, at 7 ("As technology advances, however, particularly to the point that many . . . databases become interlinked, then the threat to information privacy has the potential to increase significantly.").

> The biggest danger of biometrics, according to privacy advocates, is that biometric identifiers can be linked to databases of other information that people do not want dispersed. The threat to privacy arises from 'the ability of third parties to access this data in identifiable form and link it to other information, resulting in secondary uses of the information, without the consent of the data subject.'

Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.htm.

142. *See* Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.htm. (noting potential dangers of face recognition technology). A number of hypotheticals involving the possible use of face recognition technology have been discussed. *See* Weinstein, *supra* note 44, at 128 (noting potential abuses of technology). There is a fear that in the case of divorce, attorneys will be able to obtain information about the exact whereabouts of spouses accused of cheating. *See id.* (discussing extreme uses of technology). Many are also concerned that insurance companies will begin using the technology to track their customers and discover whether they have been taking part in potentially risky activities. *See id.* (posing potential problems from technology).

143. *See Digital Big Brother*, *supra* note 4, at C18 (noting privacy problems); *Biometrics Introduction*, *supra* note 12, at http://www.axistech.com/introduction.html (discussing use of technology in hands of third parties).

144. *See* Barber, *supra* note 2, at http://www.chipcenter. com/columns/COL_20010718.html (noting Constitution limits only government use); McCul-

laws that regulate the use of face recognition technology and laws that do control the use of an individual's private information are ill-equipped to handle this new and changing technology.[145] Without restriction, there is the potential for private use of face recognition technology to cross the boundary from providing security to invading privacy.[146] As it stands now, the use of face recognition technology does not violate the protection afforded by the Constitution. Nevertheless, there still remains an unlimited amount of danger that this technology can pose.[147]

V. THE FUTURE OF FACE RECOGNITION TECHNOLOGY AND ELECTRONIC SURVEILLANCE

A. *Expanding the Use of Face Recognition Technology*

Because of its use at the 2001 Super Bowl, Americans have become more aware of face recognition technology.[148] Since the Super Bowl, a number of cities and businesses began researching the new technology.[149]

---

lagh, *supra* note 46, at http://www.wired.com/news/print/0,1294,41571,00.html (observing Constitution only restricts actions of government, not private firms); Nuger, *supra* note 5, at http://www.engr.sjsu.edu/biometrics/publications_consideration.html (observing "[i]n the private sector, individuals will have fewer protections than in the public sector").

145. *See* Barber, *supra* note 2, at http://www.chipcenter. com/columns/COL_20010718.html ("There are no federal or state laws that limit the scope of face recognition or video surveillance that criminally punish those that violate the law or that create enforceable civil remedies for the victims of abuse.").

146. *See* O'Harrow, *supra* note 3, at A1 ("'America now faces a choice about how far we want to go down the road to being a surveillance society,' said Jeffrey Rosen, a law professor at George Washington Univerty and author of a book on privacy."); Slevin, *supra* note 4, at A1 ("'We are quickly moving to the point where law enforcement and the private sector will be able to identify us no matter where we go, no matter how anonymous we think we are . . . .'").

147. *See* WOODWARD, *supra* note 110, at 6 ("[L]aw enforcement's use of the technique at the Super Bowl does not appear to run afoul of the protections afforded by the U.S. Constitution."); McCullagh, *supra* note 46, at http://www.wired.com/news/print/0,1294, 41571,00.html ("Andrew Grosso, a former federal prosecutor, concedes that under traditional privacy law, the practice may be legal—but predicts courts will change their minds if Americans begin to object to automated sureveillance."); O'Shea, *supra* note 110, at http://www.chipcenter.com/analog/ed002?PRINT=true (declaring that face recognition technology would be considered constitutional).

148. *See* Huhn, *supra* note 4, at 51 ("Its [face recognition technology] first presence on the worldwide stage kicked off in Tampa, Fla., in January this year at Super Bowl XXXV."); Scheeres, *supra* note 42, at http://www.wired.com/news/print/0,1294,45687,00.html (noting "technology first gained public notoriety" at Super Bowl); Scheeres, *supra* note 3, at http://www.wired.com/news/print/0,1294,42317,00.html (observing face recognition technology "lept into the public's consciousness Super Bowl Sunday").

149. *See generally* Balint, *supra* note 110, at Computer Link 6 (discussing emergence of face recognition technology); Kip Bauersfeld, *A Face in the Crowd*, PRAGUE POST, Oct. 1, 2001, at eworld (same); Fiona Harvey, *Government Authorities Have Got Your Number: Surveillance Part One*, FIN. TIMES (LONDON), Oct. 2, 2001, at 13 (same); Harvey, *supra* note 123, at 14 (same); Gaetan Lecointe, *Face-recognition Software*

Additionally, a result of the terrorist attacks on September 11, 2001, airports and cities across the country are looking to use the new technology to regain a level of safety and security that seems to have been lost.[150] As a result, the biometric industry, as a whole, has experienced unprecedented growth over the past few years.[151]

Although the United States and England may lead the way in the use of face recognition technology, other countries are beginning to institute this new technology in an effort to increase security and protect their citizens.[152] While airports in the United States are just discovering the pos-

---

Gains New Popularity After US Attacks, AGENCE FRANCE-PRESSE, Oct. 3, 2001; Steven Levy, *Technology: A High-Tech Home Front*, NEWSWK., Oct. 8, 2001, at 43 (same); Rose, *supra* note 110, at Business 1 (same); *CNBC: Visionics Chairman and CEO—Interview* (CNBC television broadcast, Sept. 26, 2001) (transcript on file with author) (same); *CNN Live This Morning*, *supra* note 110 (same); *CNN: The Point with Greta Van Susteren* (CNN television broadcast, Sept. 24, 2001) (transcript on file with author) (same); *CNN Talkback Live* (CNN television broadcast, Sept. 24, 2001) (transcript on file with author) (same); *Today*, *supra* note 110 (same).

Even before the events of September 11, there were a number of airports across the country that already made use of biometric technology, primarily for the purpose of identifying their employees. *See After the Terrorist Attacks: What Could Biometrics Have Done? What Might They Do in the Future?*, Biometric Group, *at* http://www.biometricgroup.com/e/ Brief.htm (last visited Sept. 17, 2002) (reporting on previous use of technology). At eight airports across the United States and Canada, hand scans are used to allow citizens to circumvent the lines at immigration. *See id.* (listing use by airports). San Francisco International Airport also utilizes hand scans to provide employee access in the airport. *See id.* (delineating airports employing hand scans). At O'Hare Airport in Chicago, employee access to the cargo area is regulated by the use of finger scans. *See id.* (reporting on biometric technology use prior to events of September 11, 2001). Charlotte/Douglas Airport in North Carolina utilizes iris scans to regulate employee access to their cargo area. *See id.* (noting use of iris scans). Reagan National Airport in Washington, D.C. even uses fingerprint scans during employees' pre-employment background checks. *See id.* (listing airports using fingerprint scans).

150. As a result of the terrorist attacks of September 11, the U.S. government formed a number of Rapid Response Teams, one of which was designed to study airport security. *See* Mary Kirby, *Smart Card Technology on Rapid Response Team Lists*, AIR TRANSP. INTELLIGENCE, Sept. 24, 2001, at 1 (noting formation of Rapid Response Teams). The team is considering using Washington National or Boston's Logan Airport as a test case for the use of face recognition technology in an airport setting. *See id.* (reporting on suggestions of team).

151. *See* Balint, *supra* note 110, at Computer Link 6 (disclosing use of biometrics as method for identifying enemies).

152. *See* Anderson, *supra* note 4, at http://news.bbc. co.uk/hi/english/sci/tech/newsid_1500000/1500017.stm (detailing use of face recognition technology); O'Harrow, *supra* note 3, at A1 (illustrating use of technology). The use of face recognition technology is not limited to the uses described in this Comment. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (listing uses of biometrics). Throughout the United States and the rest of the world, governments and private citizens are beginning to capitalize on the security benefits they believe face recognition and biometric technology can provide. *See id.* (noting growth in use of technology).

Outside the United States, the use of face recognition technology is growing just as fast: Mexico is adapting face recognition technology to reduce voter fraud; Tokyo's subway system is equipped with a face recognition system; Germany is in-

sibilities provided by the new technology, Iceland's Keflavik International Airport has already implemented it.[153] As more countries discover the potential benefits of face recognition technology, it will likely continue to grow along with other forms of electronic surveillance.[154]

B. *Expanding Electronic Surveillance*

The increasing popularity of face recognition technology coincides with an increase in use of other forms of biometric and electronic surveillance.[155] Recently, public safety concerns have led the government to in-

stalling face recognition systems at its ATM machines; and China is using face recognition technology to allow illiterate peasants to set up bank accounts. *See id.* (listing uses of face recognition technology outside United States); Sullivan, *supra* note 110, at http://dailynews.yahoo.com/h/nm/20010808/tc/tech_privacy_surveillance_dc_1.html (exploring use in China).

153. *See CNN Live This Morning*, *supra* note 110 (discussing use of technology by Iceland).

154. *See* Balint, *supra* note 110, at Computer Link 6 (noting probable rise in revenue due to increasing popularity of biometrics); Veronica Henry, *Biometrics: Face Recognition Technology*, SANS Inst. (Mar. 12, 2001), *at* http://www.sans.org/infosecFAQ/authentic/ face_rec.htm (last visited Sept. 17, 2002) (showing rise in revenue generated by biometric technology); Emelie Rutherford, *Face Time*, DARWIN ONLINE (July 13, 2001), *at* http://www.darwinmag.com/read/machineshop/column.html?ArticleID=133 (last visited Sept. 17, 2002) (predicting rise in biometric revenue reaching $520 million by 2006). Although the exact numbers may differ, experts agree that the revenue generated by biometrics will rise dramatically in the next few years. *See* Balint, *supra* note 110, at Computer Link 6 (reporting on rise in revenue). In total, revenue generated from biometrics in 1999 was approximately sixty million dollars. *See* Henry, *supra*, at http://www.sans.org/infosecFAQ/authentic/face_rec.htm (predicting rise in revenue and analyzing revenue generated); Rutherford, *supra*, at http://www.darwinmag.com/read/machineshop/column.html?ArticleID=13 (reporting on revenue). This number is expected to rise to over five hundred million dollars in the next few years. *See* Henry, *supra*, at http://www.sans.org/infosecFAQ/ authentic/face_rec.htm (predicting future growth); Rutherford, *supra*, at http://www.darwinmag.com/read/ machineshop/column.html?ArticleID=13 (reporting on potential growth).

155. *See Today*, *supra* note 110 (observing "[w]e are rapidly becoming a surveillance society"); *Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (finding rise in surveillance). Although face recognition may currently be the most talked about form of biometric technology, it is certainly not the only form currently being used. *See id.* (describing other forms of biometric technology). Throughout the world, countries are looking to implement systems designed to increase security. *See id.* (reporting on foreign interest in biometrics). Fingerprint recognition is being implemented in a number of countries: in Japan it is being used to guard the entry to homes; customers at the Standard Bank of South Africa are now able to withdraw money from ATMs using their fingerprints; Charles Schwab is using fingerprint recognition to identify its employees; Walt Disney World is implementing a plan allowing season pass holders to do away with photo identification cards and instead use fingerprint identification. *See id.* (providing examples of biometric technology uses). ATMs in Japan are currently being equipped with iris recognition systems, while Chemical Bank is instituting a voice recognition system designed to help identify their customers. *See id.* (discussing foreign use of biometric technology). Even Mastercard and Visa are looking to utilize biometric technology to increase the security of its credit cards and reduce credit card fraud. *See id.* (illustrating uses of biometrics).

stitute a variety of surveillance mechanisms that have evoked a public backlash.[156] One of the most notable uses of surveillance is installing cameras at stoplights that are designed to catch drivers who run red lights.[157]

Another major use of electronic surveillance by the government is Carnivore, the Federal Bureau of Investigation's (FBI) new wiretapping system.[158] With a court order, the Carnivore system allows the FBI to monitor an individual's Internet use, including e-mails and websites visited.[159] Carnivore has the capacity to scan millions of e-mails per second, making it a powerful tool in the government's effort to monitor Internet traffic.[160]

Additionally, security and other concerns have motivated businesses and individuals to expand their use of electronic surveillance.[161] Recently, a number of car rental companies began installing tracking devices into their vehicles to monitor both their speed and location.[162] In New York City, taxi cab companies have installed surveillance cameras in a number of taxi cabs in an effort to eliminate crimes committed against drivers.[163] These cameras record what occurs in cabs and in the event that

156. *See* Anderson, *supra* note 4, at http://news. bbc.co.uk/hi/english/sci/tech/newsid_1500000/1500017.stm (noting protests from presence of cameras in Tampa); *Proposal Wants to Keep Big Brother's Eye Shut*, News4Jax.com, *at* http://www.news4jax.com/jax/news/stories/news-92779620010821-150801.html (last visited Sept. 12, 2002) (reporting on proposal to make face recognition technology illegal in response to unhappiness with its use in Tampa).

157. *See* Tim O'Leary, *Red-light Scofflaws Targeted*, PRESS-ENTERPRISE, Feb. 14, 2001, *available at* 112001 WL 9570130 (detailing use of cameras at traffic lights). The cameras record the license numbers of drivers who run red lights and generate tickets that are sent to the driver. *See id.* (describing how cameras work).

158. *See* Johnny Gilman, Comment, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications*, 9 COMM. L. CONSPECTUS 111, 122-24 (2001) (discussing Carnivore system and privacy implications of its use).

159. *See id.* at 112 (stating FBI's ability to use Carnivore system to monitor e-mail communication).

160. *See id.* (detailing capabilities of Carnivore system).

161. *See* Nakyanzi, *supra* note 54, at http://www.abcnews. go.com/sections/scitech/DailyNews/surveilcams010703.html (exploring debate of public safety versus personal privacy, particularly in private sector); Rutherford, *supra* note 154, at http://www.darwinmag.com/read/machineshop/column.html?ArticleID=13 (explaining private sector's use of technology).

162. *See* Robert Lemos, *Rental-car Firm Exceeding the Privacy Limit?*, CNET (June 20, 2001), *at* http://news.com.com/2100-1040-268747.html (last visited Sept. 4, 2002) (discussing rental car companies' use of tracking). The use of this tracking has caused quite a bit of controversy, and one driver who received a fine from his rental car company for speeding has since brought suit. *See id.* (noting problems stemming from use of tracking).

163. *See* Tom Jackman & Leef Smith, *Taxi Camera Develops Its First Lead for Police; Armed Robbery in Mount Vernon Caught in Digital Clarity*, WASH. POST, Aug. 22, 2001, at B1 (detailing use of cameras in taxis in response to robberies). Since June, 2001, the 107 taxi cabs operated by Springfield Yellow Cab in Northern Virginia have been equipped with small cameras mounted near the cars' rearview mirrors. *See id.* (illustrating success of cameras in identifying criminals). The cameras are designed to cut down on the number of crimes committed against taxi cab

a crime does occur, they provide evidence to assist in tracking down the criminals.[164] These are only a few examples of how the government and private citizens are expanding the different forms of electronic surveillance to monitor the actions of others.[165]

C. *Regulating Electronic Surveillance*

One of the most significant problems with the already existing face recognition systems is the lack of laws or regulations setting guidelines for their uses.[166] As discussed previously, while its use may be protected by the Constitution, there still remains a need to regulate biometric technology.[167] Many people believe that the use of the technology may infringe on individuals' privacy rights.[168]

---

drivers, a major issue for the profession in the past few years. *See id.* (noting goal of cameras). The cameras are designed to take photographs when the cab door is opened, when the meter is activated and again at random intervals, as well as to have the capability to take photos manually. *See id.* (discussing operation of surveillance cameras). Each camera stores up to 320 photographs, and they are reviewed only if a crime has been committed. *See id.* (detailing capabilities of cameras). The use of cameras in taxi cabs began in Houston, Texas in 1999 and cameras have been installed in taxi cabs in Austin, Denver, Jacksonville, Minneapolis, San Antonio and New York, as well as those in Northern Virginia. *See id.* (recognizing expanding use of cameras in taxi cabs). With a rise in the number of crimes committed against taxi cab drivers, some areas have required the presence of these cameras, with Washington D.C. requiring all taxi cab drivers to have the cameras installed in their cars. *See id.* (reporting on required presence of cameras).

164. *See id.* (describing capabilities of system). One example of the benefits of these surveillance cameras is in the case of a taxi cab driver in Mount Vernon, Virginia who was robbed while on duty. *See id.* (outlining facts of incident). Because the taxi cab was equipped with a surveillance camera, the police have been able to produce clear, sharp pictures to aid in their search for a suspect. *See id.* (noting ability of cameras to aid in search for suspect).

165. *See id.* (exploring use of cameras in taxi cabs); Lemos, *supra* note 162, at http://news.com.com/2100-1040-268747.html (discussing use of tracking by rental car companies).

166. *See* Ken Phillips, *Unforgettable Biometrics*, ZDNet (Oct. 26, 1997), *at* http://www.zdnet.com/eweek/reviews/1027/27bioapp.html (last visited Sept. 4, 2002) ("The main challenges currently facing the biometric industry are not technological, but rather a lack of standards and law of public awareness.").

167. *See* Greene, *supra* note 110, at http://www. theregister.co.uk/content/6/20966.html ("'By implementing reasonable safeguards [for government use of biometric face scanning], we can harness its power to maximize its benefits while minimizing the intrusion on individual privacy.'").

168. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998) (discussing impact of technology on privacy rights); *see also Digital Big Brother*, *supra* note 4, at C18 ("'Privacy is going to become the civil rights issue of this decade,' said Rep. Edward Markey, D-Mass., a member of the congressional privacy caucus formed last year."); Givens, *supra* note 12, at http://www.privacyrights.org/ar/Privacy-Issues-List.htm (observing "facial recognition biometrics is one of the most alarming because it can be deployed secretly").

Another issue concerning the use of face recognition technology is what happens with all of the information that is gathered.[169] Although the government currently maintains that it automatically discards all faces that are not a match, there is growing concern that, with the expanding technology, the government will begin maintaining files on all of the faces scanned into the databases.[170]

The same fears of information gathering are even more prevalent when face recognition technology makes its way into the hands of private citizens.[171] Many have expressed concern that in the hands of private citizens, face recognition technology will allow the general public to maintain vast databases of information on individuals, retrievable the moment a face is scanned and a match is made.[172] This technology has the potential to allow third parties to monitor constantly the movements of individuals, thereby affording them no privacy.[173]

This concern over the lack of regulation led to the Congressional Privacy Caucus, formed in an effort to discuss and investigate current privacy issues, with a focus on maintaining personal privacy.[174] Even individuals in the industry have raised this concern over a lack of individual privacy. At least one maker of face recognition technology has called for the regulation of its use, focusing on notifying individuals that they are being monitored.[175]

---

169. *See* WOODWARD, *supra* note 110, at 13 (disclosing that much more private information is collected and revealed to government entities than is necessary to achieve purpose of surveillance).

170. *See id.* (analyzing government's need to regulate how long it maintains photos in system before discarding).

171. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (discussing technology in hands of third parties); *Digital Big Brother*, *supra* note 4, at C18 ("The threat to privacy arises [from] . . . the ability of third parties to access this [personal information] . . . .").

172. *See Biometrics Introduction*, *supra* note 12, at http://www.axistech.com (observing that threat to privacy arises from ability of third parties to use this technology); *Digital Big Brother*, *supra* note 4, at C18 (discussing potential abuses of technology).

173. *See* WOODWARD, *supra* note 110, at 7 (divulging fears of "tracking and clandestine capture").

174. *See* Senator Richard C. Shelby, *Shelby Announces Formation of Congressional Privacy Caucus*, InCongress (Feb. 11, 2000), *at* http://fs.huntingdon.edu/jlewis/FOIA/Privacy/Sen-Shelby-Privacy-Caucus-prsrs314.htm (last visited Sept. 4, 2002) (explaining formation of caucus).

175. *See On the Law Enforcement Alliance of America's Opposition to Face Recognition Software*, Law Enforcement Alliance of Am. (July 3, 2001), *at* http://www.notbored.org/leaa.html (last visited Sept. 5, 2002) (discussing call for regulation).

In September 1998, the International Biometric Industry Association (IBIA) was formed and currently has a membership of twenty-seven companies. *See Biometrics and Privacy: Industry Policy on Crowd Surveillance*, *supra* note 110, at http://www.ibia.org/pressrelease19.htm (outlining formation of IBIA). The organization is open to all manufacturers and users of biometric technology who "agree to abide by the IBIA Statement of Principles and Code of Ethics." *Id.* On March 24, 1999, IBIA adopted a set of privacy principles that were aimed at encouraging

Congress must establish a set of guidelines that regulate the use of this technology by both the government and private citizens.[176] As the makers of the technology have recognized the need for regulation, there is no doubt that the legislature is not far behind.[177] Furthermore, although the use of face recognition technology remains untested in the court system, its expansion virtually assures that it will not remain untested for long.[178]

VI. CONCLUSION

As early as 1963, the late Supreme Court Justice William J. Brennan, Jr. "warned that 'electronic surveillance makes the police omniscient, and police omniscience is one of the most effective tools of tyranny.'"[179] With the development of face recognition technology, and the capabilities it possesses, an issue arises as to whether the Constitution is equipped to

---

biometric manufacturers and users to take steps to secure the data collected by biometric systems. *See id.* (exploring privacy principles). These guidelines are designed to apply to manufacturers, customers and users of the new technology. *See id.* (disclosing goal of guidelines). The guidelines are:

1. Biometric data is electronic code that is separate and distinct from personal information, and provides an effective, secure barrier against unauthorized access to personal information. Beyond this inherent protection, IBIA recommends safeguards to ensure that biometric data is not misused to compromise any information, or released without personal consent or the authority of law.
2. In the private sector, IBIA advocates the development of policies that clearly set forth how biometric data will be collected, stored, accessed, and used, and that preserve the rights of individuals to limit the distribution of the data beyond the stated purposes.
3. In the public sector, IBIA believes that clear legal standards should be developed to carefully define and limit the conditions under which agencies of national security and law enforcement may acquire, access, store, and use biometric data.
4. In both the public and private sectors, IBIA advocates the adoption of appropriate managerial and technical controls to protect the confidentiality and integrity of databases containing biometric data.

Id.

176. *See* WOODWARD, *supra* note 110, at 13 (calling for "specific protocols" regarding use of this new technology); Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.htm (describing need for regulation of technology).

177. *See* WOODWARD, *supra* note 110, at 13 (stressing need for "strict controls to safeguard information"); Prevost, *supra* note 6, at http://www.swiss.ai.mit.edu/6.805/student-papers/fall99-papers/prevost-biometrics.htm ("What is needed is for policy makers . . . and engineers of biometric systems . . . to collaborate . . . .").

178. *See* Kasindorf, *supra* note 4, at A3 (observing face recognition technology remains untested in court); Barber, *supra* note 2, at http://www.chipcenter. com/columns/COL_20010718.html (highlighting that Fourth and Fifth Amendments, which protect against unreasonable searches and seizures and self-incrimination, have never been invoked against blanket surveillance of whole population).

179. Diana Ray, *Big Brother Is Watching You*, INSIGHT ON NEWS, July 23, 2001, at 18.

protect Americans adequately against such tyranny.[180] The unique characteristics of this technology make it difficult to apply existing case law in order to determine its legality.[181] Although the Constitution was drafted in such a way that it allows the law to metamorphasize as society and technology advance, case law has yet to address the unique problems face recognition technology raises.[182]

In the hands of the government, face recognition technology may be the most cutting edge way for police to track criminals and terrorists, but in the hands of individual citizens, this technology presents a variety of privacy issues including access to personal information and the ability to track or pinpoint an individual's movements.[183] In the end, when deciding whether face recognition technology is constitutional, citizens and the courts may be forced to weigh their desire to feel secure in their own homes against the value they place on their privacy.[184]

Bridget Mallon

---

180. *See generally* Alexander T. Nguyen, Comment, *Here's Looking at You Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2 (2002) (analyzing problems created by face recognition technology).

181. For a discussion of the existing case law, see *supra* notes 76–109 and accompanying text.

182. *See* Barber, *supra* note 2, at http://www.chipcenter.com/columns/COL_20010718.html (identifying "no laws on the books" and no legal remedies in courts); Nuger, *supra* note 5, at http://www.engr.sjsu.edu/biometrics/publications_ consideration.html (commenting that this new technology has yet to be addressed in court).

183. *See* WOODWARD, *supra* note 110, at 7 (analyzing issues surrounding face recognition technology); Givens, *supra* note 12, at http://www.privacyrights.org/ar/Privacy-IssuesList.htm (analyzing face recognition technology).

184. *See CNN Live This Morning*, *supra* note 110 (discussing privacy concerns surrounding face recognition technology). Although the issue has not yet been addressed by the courts, some have already considered the possible conflicts. *See id.* (noting problems arising from use of technology). Addressing a law school in New York, Supreme Court Justice Sandra Day O'Connor asked "when does the legislation that we pass to hinder terrorism become so overwhelming that it takes away our civil liberties . . . this is what we have to be on the look out for." *Id.*