UIC John Marshall Journal of Information Technology & Privacy Law

Volume 20
Issue 3 *Journal of Computer & Information Law - Spring 2002*

Article 5

Spring 2002

O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology, 20 J. Marshall J. Computer & Info. L. 471 (2002)

Susan McCoy

COMMENT

O'BIG BROTHER WHERE ART THOU?: THE CONSTITUTIONAL USE OF FACIAL-RECOGNITION TECHNOLOGY

I. INTRODUCTION

"Privacy is dead, deal with it."[1]

The availability of privacy has diminished in this technological era. Furthermore, it has been questioned if it is even possible to maintain privacy in an age where our daily actions can be monitored.[2] Should we limit our expectations of privacy in order to form a more secure and safe lifestyle?

Legal scholars advocating privacy from surveillance systems often illustrate their point with hypothetical Orwellian societies that criticize the mass surveillance of common activities by Big Brother.[3] For a contrary point of view, imagine the type of society for which they advocate. For example, while strolling in the park with your daughter, she asks to play on the swing set at the park's playground. You give in, as she knew you would, and while she swings you notice momentarily that the leaves on the trees are changing color earlier than ever this year. Looking back with the expectation of seeing your daughter in mid-flight laughing, you only see the soft swaying of the swing and no sign of your giggling little girl. "I only took my eyes away from her for a second," you declare to the police officer hysterically as he tells you a witness saw her leave with a middle-aged man, but could not make out a description.

How do privacy rights outweigh the benefits of Biometric technology, or specifically, video surveillance with facial-recognition technology, in

1. *See* Brock N. Meeks, *Is Privacy Possible in the Digital Age?* ¶ 1 <http://stacks.msnbc.com/news/498514.asp> (accessed Dec. 7, 2000) (quoting Scott McNealy, Sun Microsystems CEO).

2. *See id.*

3. *See* Christopher Milligan, *Facial Recognition Technology, Video Surveillance and Privacy*, 9 S. Cal. Interdis. L.J. 295, 296 (1999) (referring to "Orwellian Reflections" in the title of the article's subsection); George Orwell, *1984* (New Am. Lib., Inc., 1961).

the above scenario?[4] In a quasi-Orwellian society,[5] the surveillance system would have observed everything from the first big push you gave your daughter on the swing, to the pondering look on your face as you sat on the bench gazing at the trees. More importantly, surveillance would have captured on video the middle-aged man who asked your little girl to help him find his lost puppy. In that society there would be a database of known sex offenders and other criminals, along with their pictures, so that seconds after making the request to identify the unknown man, facial-recognition software would provide you with all the information necessary to find your daughter as quickly as possible.

The use of facial-recognition technology does not violate Fourth Amendment rights to privacy.[6] This Comment will explore the dueling arguments of privacy and safety relative to the implementation of facial-recognition technology. Section II of this Comment will outline a brief history and explanation of facial-recognition technology and the relevant case law on this issue. Section II also illustrates the debate between privacy protection and the need for expedient and more accurate security measures to protect against criminal activity and terrorist attacks. Section III will establish that the implementation of facial-recognition technology does not violate privacy rights. Additionally, that section will propose laws for future legislation on this topic to allow this technology to be implemented in both private and public sectors, while concurrently safeguarding citizens' privacy rights.

4. Another very real scenario is when known terrorists are allowed access and entrance onto planes because there are no video surveillance systems, which are sophisticated and fast enough to spot these dangerous people in a crowd, and no accessible database of such perpetrators in order to identify them. *See generally* CNN, *Gideon Rose: Why Did September 11 Happen?* <http://www.cnn.com/2001/COMMUNITY/11/26/rose/index.html> (accessed Nov. 26, 2001) (discussing, generally, the terrorist attacks of Sept. 11, 2001).

5. Quasi-Orwellian society refers to a society that uses facial-recognition technology while, at the same time, remaining mindful of a person's right to privacy where that expectation is reasonable. *See generally Katz v. U.S.*, 389 U.S. 347 (1967).

6. The Fourth Amendment of the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

II. BACKGROUND

A. FACIAL-RECOGNITION TECHNOLOGY

1. *Biometrics Generally*

Facial-recognition technology is a division of Biometric technologies. Biometrics was developed in the 1990's at the Massachusetts Institute of Technology.[7] It is the science of analyzing and measuring physiological data or "the identification of people by their unique features."[8] Biometrics uses an individual's inimitable and distinguishable features and compares them with databases of other similar physiological characteristics[9] for such purposes as security clearance in corporate and governmental buildings, identifying perpetrators of illegal acts, or locating missing children. Biometrics is divided and categorized by what specific physical characteristic it was programmed to observe.[10] Some of the more familiar systems are finger imaging,[11] hand geometry,[12] voice au-

---

7. *See* Vickie Chachere, *Snooper Bowl? Biometrics Used at the Super Bowl to Detect Criminals in Crowd* ¶ 6 <http://acbnews.go.com/sections/scitech/DailyNews/superbowl_biometrics_010213.html> (accessed Feb. 13, 2001).

8. *See* Casino Mag., *Trends: Face-Recognition Raises Fears of Big Brother* ¶ 25 <http://www.casinomagazine.com/managearticle.asp?c=570&a=13> (accessed Sept. 27, 2001). Biometrics has become the most innovative and sophisticated solution to determine identification in the world. Strategic Research Inst., *Successful Strategies For Rolling Out Biometrics Technology* ¶ 3 <http://www.srinstitute.com/part_iter_site_page.cfm?iteration_id=279> (accessed Oct. 31, 2001). Actually, there are expectations that the Biometrics market will be a multi-billion dollar business within the next five years. *Id.*

9. *See* Benjamin Pimentel & Benny Evangelista, *Tech v. Terrorism: Airports Looks To New Technologies To Beef Up Security* ¶¶ 12, 24 <http://www.sfgate.com/cgibin/article.cgi?file=/chronicle/archive/2001/09/17/BU190282.DTL> (accessed Sept. 17, 2001). Biometric technology used in conjunction with other airport security measures would be a beneficial tool in keeping our skies safe. *Id.* at ¶¶ 11, 23.

10. In a 2002 Biometric Market Report, facial-recognition technology represented 12.4% of the market in a comparative market share by technology analysis. Intl. Biometric Group, *Biometric Market Report 2003-2007* § 2 <http://www.ibgweb.com/reports/public/market_report.html> (accessed Oct. 2, 2002). Facial-recognition technology is expected to reach $200 million in annual revenues in 2005. *Id.* This figure is below the finger-scan system, which is estimated to control more than half of the market share. *Id.* Fourth in line for market share, after facial-recognition technology, is the hand scan at ten percent of the market share. *Id.* The government will be responsible for generating $1.2 billion in annual revenues for the biometrics industry over the next five years, thereby making it the leader in the biometrics vertical market. *Id.*

11. *See* Ellen Messmer, *Special Focus: Is Biometrics Ready To Bust Out?* § 25 <http://www.nwfusion.com/news/2002/1007specialfocus.html> (accessed Oct. 7, 2002). A computer scans the finger and reveals individual patterns, much like an ink fingerprint. *Id.* Seven United States airports have implemented or have ordered fingerprint-scanning systems, which will be used to provide authorized airport personnel access to high security areas. Pimentel, *supra* n. 9, at ¶ 15.

12. *See* Messmer, *supra* n. 11. The hand is placed on the flat surface of a scanner where ninety points of the hand are analyzed, such as the shape of the knuckle and dimen-

thentication,[13] facial-recognition,[14] retinal scanning,[15] and iris scanning.[16] Additionally, other lesser-known types of biometrics, which are still in the development stage, are body odor,[17] gait-recognition,[18] facial-thermography,[19] and ear shape.[20]

2. *Implementation of Facial-Recognition Technology*

In the growing field of Biometrics, facial-recognition technology has taken video surveillance into the future.[21] The fundamental principle

---

sions of the finger. *Id.* Individuals who travel frequently can register their palm prints with Immigration and Naturalization Services and bypass immigration proceedings at almost a dozen North American airports. David George, *Face Recognition May Enhance Airport Security* ¶ 10 <http://www.cnn.com/2001/US/09/28/rec.airport.facial.screening/index.html> (accessed Sept. 28, 2001).

13. *See* Messmer, *supra* n. 11. Voiceprints are created with a person's unique inflection and the individual highs and lows of their voice. *Id.* This biometric is useful in telephone-based procedures. *Id.*

14. *See id.* The system encodes specific measurements of distances between facial features through video surveillance. *Id.*

15. *See id.* The retina, similar to a fingerprint, is unique to each person and the scanning technology encodes its distinctive capillaries. *Id.*

16. *See id.* Iris pattern and color are mapped after a video image of the eye is taken. *Id.* In Charlotte, North Carolina, the airport tested eye-recognition technology on more than 6,000 applications of people who previously consented to "eye prints." George, *supra* n. 12, at ¶ 8. The experiment proved to be one hundred percent accurate. *Id.* The airlines believe that expediting known passengers through the airport allows law enforcement officers and security officials to dedicate more time and scrutiny to suspicious and potentially dangerous travelers. *Id.* at ¶ 9.

17. *See* Ursula Masterson, *Biometrics and the New Security Age* § 10 <http://www.angelfire.com/nt/selcukgun/en/tran_2.htm> (accessed Oct. 25, 2002) (analyzing the chemical blueprint of the smell of the human body).

18. *See id.* (recognizing the manner in which an individual walks or runs).

19. *See id.* (illustrating that each individual's flow of blood under the skin is distinctive and the technology analyzes the patterns made by the facial heat).

20. *See id.* (measuring the bone structure and shape of the ear).

21. Video surveillance technology, without the face-recognition software, is currently being used in the majority of the private sectors in the country, such as banks, convenient stores and even school systems. SLStreaming, *Surveillance Cameras on School Campuses* ¶ 1 <http://www.hometoys.com/releases/apr01/slstream01.htm> (accessed Apr. 9, 2001). For example, surveillance cameras, called C-Cams, are placed in schools and then monitored from the Internet in an effort to deter violence in the school systems and lessen police response time to the facility. *Id.* at ¶¶ 6, 8; *see generally* Roy Huntington, *Streaming Video-A Co's new Best Friend?* ¶ 2 <http://www.policemag.com/t_cipickcfm?rank=10> (accessed Oct. 7, 2002). Likewise, law enforcement agencies across the country also utilize video surveillance systems to patrol intersections and highways. Associated Press & Reuters Ltd., *Seeing Red Over Traffic Light Cameras* ¶ 3 <http://www.cbsnews.com/stories/2001/07/31/national/printable304257.shtml> (accessed July 31, 2001). Once police surveillance cameras have captured a driver running a red light or speeding, the plate numbers from the photos are researched to find the owner's address and then citations are mailed to the respective locations. *Id.* Safety studies illustrate that such procedures have actually reduced the number of accidents in the fifty cities across the country that are currently using

behind facial-recognition technology is that each person's face can be numerically coded and then compared to a database of thousands of other identities of either known criminals or authorized personnel, in nearly real-time.[22] The additional security is a barrier which known or suspected criminals have to cross, giving law enforcement better opportunities to catch these individuals.

Facial-recognition software is an unobtrusive means to verify authorization of individuals entering corporate and governmental buildings or high security facilities.[23] The installation of a facial-recognition system is also a simple procedure because most companies and corporate buildings have already integrated cameras into their security plans and procedures. Moreover, the majority of these facilities keep pictures of their employees and residents on file.[24]

Face-recognition technology has been a work in progress for university scientists over the past decade.[25] Initially, the U.S. Defense Department was funding the research to be used in identifying criminals as they crossed borders into this country.[26] However, the majority of fund-

---

video surveillance. *Id.* at ¶ 4. In addition to making the roads safer, video surveillance systems are less expensive than placing police officers at problem traffic and speeding areas. *Id.*; *Vt. v. Costin* is a Vermont Supreme Court case that held the use of video surveillance was not unconstitutional. *Vt. v. Costin,* 168 Vt. 175 (Vt. 1998). In this case the State Police discovered marijuana plants on the defendant's unenclosed property, along with a footpath connecting the residence on the property and the plants. *Costin*, 168 Vt. 176. The officers then installed a video camera less than seventy-five feet from the plants. *Id.* The video showed the defendant cultivating the marijuana plants and was later arrested. *Id.* The defendant argued that the warrantless use of video surveillance was unconstitutional. *Id.* The Supreme Court of Vermont held that a person would not have more protection from electronic surveillance on his private and open land than he would if he was under surveillance in a public place. *Costin*, 168 Vt. 179. The electronic surveillance did not make available information, which could not have been observed by the naked eye. *Costin*, 168 Vt. 180-81. The Court held that the electronic surveillance was merely a substitute for a stakeout by a police officer and was even less intrusive. *Costin*, 168 Vt. 181.

22. Chachere, *supra* n. 7, at ¶ 7. Facial-recognition is a system that crosschecks footage retrieved from surveillance cameras with a database compiled of mugshots of known criminals. Andy Sullivan, *Interest In Face Scanning Grows After Attacks* ¶ 2 <http://www.siliconinvestor.com/stocktalk/msg.gsp?msgid=16375863> (accessed Sept. 18, 2001). This technology is also applicable to objects other than a person's face, however it is not used as widely. PR Newswire, *Imagis ID-2000 Biometric Facial Recognition Technology Has One-of-a-Kind Features for Identifying Faces & Images* ¶ 2 (Sept. 25, 2001) (available in LEXIS, News library, Individual Publication file). For example, the software can compare other identifiable marks such as tattoos, scars, and jewelry. *Id.*

23. Emelie Rutherford, *Facial-Recognition Tech Has People Pegged* ¶ 6 <http://www.cnn.com/2001/TECH/ptech/07/17/face.time.idg/index.html> (accessed July 17, 2001).

24. *Id.* The pictures taken are for key cards or passes for the purposes of entry into a building or a secured area of a facility. *Id.*

25. *Id.* at ¶ 4.

26. *Id.* Border crossing identification cards are documents used for legal aliens to cross the border into the United States. 8 U.S.C.S. § 1101(A)(6) (2000). Regulations require that

ing for the technology is now being fueled by commercialization of the software to private sectors and local governments.[27]

Facial-recognition software became famous when it was implemented at the 2001 Super Bowl in Tampa as an experiment and resulted in the coining of the "Snooper Bowl."[28] The technology was used to search and identify felons and terrorists in a crowd of a hundred thousand.[29] Since then many different corporations and event sponsors have been contemplating the idea of incorporating facial-recognition software into their security procedures.[30]

3. *Developmental Markets*

There are several Biometrics corporations with facial-recognition technology on the market,[31] and this Comment will address two of them and how they have designed their respective software.[32] First, Visionics,

---

before an alien can enter the country he must have an identification card, which contains a biometric identifier, like fingerprints or handprints, and the alien must match the characteristic specific to his identification card. *Id.*; *see* Joris Evers, *Dutch Government Turns to Biometrics to ID Immigrants* ¶ 7 <http://www.idg.net/crd_idgsearch_514762.html> (accessed Apr. 18, 2001) (explaining how, by 2003, all Dutch citizens will have their individual biometrics data stored on a chip in their European Union identification cards).

27. Rutherford, *supra* n. 23, at ¶ 3; *see generally* Casino Mag., *supra* n. 8, at § 11. The majority of the casino industry put the software into operation in 1997 to spot known card sharks. *Id.* Additionally, testing of the facial-recognition software has also been considered in some U.S airports. George, *supra* n. 12, at ¶ 1.

28. Chachere, *supra* n. 7, at ¶ 2. The nickname Snooper Bowl refers to the dislike of the technology by insinuating that it is invasive and excessively intrudes into private acts. *Id.* Facial-recognition software was also employed in Tampa's nightlife district, Ybor City, where the law enforcement agency had been using video surveillance without the technology for many years. *Id.* at ¶ 15.

29. *Id.* at ¶ 1. Although no one was arrested that day, nineteen people were identified with outstanding warrants for minor offenses. *Id.* at ¶ 11.

30. As authorized by the Legislature, the Department of Motor Vehicle in Colorado is continuing with compiling their own database containing digital three-dimensional maps of faces of those individuals who are requesting driver's licenses. Am. Civ. Liberties Union Freedom Network, *Proliferation of Surveillance Devices Threatens Privacy* ¶ 4 <http://www.aclu.org/ news/2001/n071101a.html> (accessed July 11, 2001). Additionally, even though the American Civil Liberties Union has requested a ban be placed on facial-recognition technology at future football games, security personnel for the Winter Olympics in Salt Lake deliberated the use of the technology. Lavonne Kuykendall, *Security Failure Is Biometrics' Gain*, Am. Banker ¶ 9 (Sept. 20, 2001) (available in LEXIS, News library, Individual Publication file).

31. There are over twenty facial-recognition development groups on the market along with numerous Internet resource sites and research groups. Intl Biometrics Group, *supra* n. 10, at § 1; Face Recognition Home Page, *Research Groups, Commercial Products* §§ 2, 6 <http://www.cs.rug.nl/~peterkr/FACE/face.html> (accessed Oct.21, 2002).

32. At Boston's Logan Airport, both Visionics and Viisage are bidding on the facial-recognition software contract. *See* Raphael Lewis & Ross Kerber, *Logan Will Test Face-Data Security* ¶ 6 <http://www.boston.com/dailyglobe2/298/metro/Logan_will_test_face_

the creator of the FaceIt system, got its start from mathematical research conducted at Princeton University's Institute for Advanced Study.[33] The FaceIt system measures the face's nodal points, sometimes called landmarks, which are the peaks and valleys inherent to a person's face.[34] The software plots the relative positions of the nodal points in order to derive a series of numbers, called a faceprint.[35] The program then compares the faceprint to other identities compiled in a file.[36] Visionics has determined that the face has eighty nodal points, but its software only needs fourteen to twenty-two points in order to complete recognition of an individual's unique facial pattern.[37]

The primary area of concentration for this technology is referred to as the "golden triangle".[38] The triangle is formed by the distance between the temples and to the lips, mostly incorporating the inner region of the face.[39] The basis for this particular type of analysis rests on the belief that this region of the face is unlikely to change with a disguise, additional weight, or even age.[40]

Another company developing facial-recognition software is Viisage Technology of Massachusetts.[41] Viisage's facial-recognition technology is called Facefinder and differs somewhat from Visionics technology.[42] Facefinder technology was founded on the idea that each individual's face differs slightly from one of a hundred and twenty-eight compiled "standard" faces.[43] A person's face is given a numerical code called the eigenface.[44] The eigenface is derived from a digital picture and then

---

data_security+.shtml> (Oct. 25, 2001). Both companies will install their own systems in the airport for a test period of ninety days. *Id.* at ¶ 8.

33. Casino Mag., *supra* n. 8, at ¶ 26. Visionics has also created a smart card system that stores an individual's faceprint on an identification card and is employed without the use of cameras. Rutherford, *supra* n. 23, at ¶ 9. The smart card would be swiped through a door as a key-pass or a security precaution. *Id.*

34. *Id.* at ¶ 8. Examples of nodal points on the face are the nose, the eye sockets, and the cheekbones. *Id.*

35. *Id.* at ¶ 9.

36. *Id.*; Casino Mag., *supra* n. 8, at ¶ 30 (illustrating how Visionics is sharing a database with Interpol, the international police organization, that stores information on terrorists and criminals).

37. Rutherford, *supra* n. 23, at ¶ 8; George, *supra* n. 12, at ¶ 4.

38. Rutherford, *supra* n. 23, at ¶ 8.

39. *Id.*

40. *Id.* Other divisions of Biometrics have the potential for fraud. *Id.* For example, scars may distort finger and hand prints and a person's voice can be altered or imitated easily. *Id.*

41. Casino Mag., *supra* n. 8, at ¶ 28.

42. Chachere, *supra* n. 7, at ¶ 10.

43. *Id.* at ¶ 7; Casino Mag., *supra* n. 8, at ¶ 28.

44. Viisage Tech., *Technology* ¶ 1 <http://www.viisage.com/technology.htm> (accessed Oct. 2, 2002).

compared to a database of millions of other eigenfaces.[45] Once a match is made, the software is designed to send a warning that a potentially dangerous person has been identified.[46]

Viisage markets its facial-recognition technology as a cost effective, non-invasive, and accurate tool for improved security, identification protection, and fraud reduction.[47] The company provides a wide selection of systems and types of software in order for a company or facility to build the appropriate security system for its respective security needs and environment.[48] Currently, the Company has customers across a wide spectrum of organizations,[49] such as Social Services to prevent double dipping into Welfare,[50] Automated Teller Machines,[51] Correction Facilities,[52] and the Illinois State Police in order to detect and identify driver's license fraud and other criminal activities.[53]

Compared to other types of Biometric technologies, facial-recognition systems are more likely to be widely accepted due to its non-invasive character and low rate of error, which is less than one percent.[54] Al-

45. *Id.* Viisage software can be applied to databases containing millions of faces or eigenfaces and still find a match in a matter of seconds. *Id.*

46. Chachere, *supra* n. 7, at ¶ 8. Also, if a match is completed, the authorized individual seeking access into a secured area will have permission to enter. *Id.*

47. Viisage Tech., *Products and Services* § 2 <http://www.viisage.com/product.htm> (accessed Sept. 28, 2001).

48. *Id.* at § 1.

49. Viisage Tech., *FR Customers* § 1 <http://www.viisage.com/frcustomer.htm> (accessed Sept. 28, 2001).

50. Viisage Tech., *FR Services: Social Services, Massachusetts Department of Transitional Assistance* § 1 <http://www.viisage.com/frcustmassach.htm> (accessed Oct. 3, 2001). Massachusetts has a database of over five hundred thousand images, which each new applicant for financial assistance is compared against. *Id.* The FaceEXPLORER system generates a list of duplicate matches, which are then investigated further for fraud. *Id.*

51. Viisage Tech., *FR Customers: ACM/ATM, Global Cash* ¶ 1 <http://www.viisage.com/frcustglobal.htm> (accessed Oct. 3, 2001).

52. Viisage Tech., *FR Customers: Corrections, Wisconsin's Department of Corrections* § 1 <http://www.viisage.com/frcustwisconsin.htm> (accessed Oct. 3, 2001).

53. Viisage Tech., *FR Customers: State Police/DMV, Illinois Secretary of State and State Police* ¶ 1 <http://www.viisage.com/frcustillnois.htm> (accessed Oct. 3, 2001). Currently, Illinois has the world's first large scale driver's license facial-recognition system which has a database of more than four million images and an expected growth of twenty million. *Id.* The system offers two different methods of operation called "batch" and "fast-response." *Id.* The "batch" method generates a list for the Secretary of State to investigate cases most likely to be fraudulent. *Id.* "Fast-response" is an investigative tool used by the Secretary of State and the State Police to perform specific individual searches to identify unknown suspects or victims. *Id.*

54. Rutherford, *supra* n. 23, at ¶ 6. Logan Airport, in Boston, is planning on being one of the first airports in the United States to incorporate facial-recognition technology into its security procedures. Lewis, *supra* n. 32. The airport will be comparing the faces of travelers with a database of suspected terrorists. *Id.* at ¶ 9. Iceland's Keflavik Airport was the first to announce that it was implementing facial-recognition software to screen its passen-

though other biometric systems have an even lower error rate, such as iris scanning, face-recognition technology does not require active participation from the user.[55] Additionally, in the event a backup system is needed, facial-recognition technology has a natural inherent support based on our own ability to recognize each other.[56]

B. Relevant Case Law on Surveillance Technology and Privacy

The Fourth Amendment[57] disallows unreasonable searches and seizures.[58] An unreasonable search arises when an individual's reasonable expectation of privacy is encroached upon.[59] This Comment explains that the implementation of facial-recognition technology is not a search prohibited by the Fourth Amendment because it does not violate reasonable expectations of privacy.[60]

There are few principal cases involving privacy and the use of electronic surveillance. The first is *Katz v. U.S.* where the Supreme Court held that the Fourth Amendment "protects people and not places."[61] In *Katz*, an individual was convicted of violating a federal statute by trans-

---

gers and many more airports are expected to follow suit. *Id.* at ¶ 4; George, *supra* n. 12, at ¶ 2.

55. Rutherford, *supra* n. 23, at ¶ 6; Viisage Tech., *Products and Services: Facefinder* § 2 <http://www.viisage.com/facefinder.htm> (accessed Sept. 28, 2001).

56. Rutherford, *supra* n. 23, at ¶ 7. For example, most companies and organizations require employees and members to wear identification badges with the individual's picture. Security personnel could rely on this as verification for admittance in backup procedures.

57. U.S. Const. amend. IV.

58. Kent Greenfield, *Cameras in Teddy Bears: Electronic Visual Surveillance and the Fourth Amendment*, 58 U. Chi. L. Rev. 1045, 1049 (1991). If a search is required then law enforcement must obtain a warrant. *Id.* Warrants are only authorized upon a showing of probable cause that there is a substantial possibility that evidentiary items can be found at a certain place at a certain time. *Id.* However, the use of facial-recognition technology is unlikely to fall under the requirement of obtaining a warrant because law enforcement would already know the identity of the suspect. Milligan, *supra* n. 3, at 318. Furthermore, facial-recognition is not a search disallowed under the Fourth Amendment. *Id.*

59. Greenfield, *supra* n. 58, at 1049; *Winston v Lee*, 470 U.S. 753 (1985) (illustrating that an individual cannot be forced by the state to undergo surgery to remove a bullet because surgery would be so invasive, and, thus, unreasonable even if likely to hold some evidentiary value and supported by a court order).

60. There is a limited expectation of privacy in public places. Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079, 1088-89 (1997). Facial-recognition will be implemented in public places. Thus, the implementation of facial-recognition will not violate privacy rights because of the limited expectation of privacy rights in public places. *Id.*

61. *See Katz v. U.S.*, 389 U.S. 347 (1967); William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 Kan. L. Rev. 1 (1974). Rehnquist believes that privacy rights have no position in public places, especially when balanced against law enforcement needs. *Id.* at 2. He also wrote that driving in a car down a public street is not a private act. *Id.* at 9.

mitting wagering information by telephone.[62] FBI agents wiretapped a public telephone booth that the defendant used to make the calls.[63] The Supreme Court decided that a person who used a telephone booth and closed the doors behind him was entitled to protection under the Fourth Amendment for his conversation and that a warrant should have been obtained.[64] After *Katz*, the test for determining if privacy was invaded unconstitutionally was based on whether the individual had a reasonable expectation of privacy and whether society would recognize that expectation as reasonable.[65]

The most recent case about the constitutional use of technology in warrantless searches is *Kyllo v. U.S.*,[66] which narrowed the expectation of privacy test from *Katz*.[67] The government suspected Danny Kyllo of

---

62. *See Katz*, 389 U.S. 348.

63. *See id.*

64. *See Katz*, 389 U.S. 352. By closing the telephone booth door behind him, Mr. Katz was able to show that he did not want anyone to hear him and, therefore, that he had an expectation that his phone conversation would be private. *Id.*

65. *See Katz*, 389 U.S. 352, 355; Burrows, *supra* n. 60, at 1088. In *United States v Knotts*, 460 U.S. 276 (1983), law enforcement officials placed a beeper in a container of chloroform, which is used to make illegal drugs. *Id.* The police used the beeper to determine the changed location of the container. *Id.* The Court held that monitoring by beeper was not a search prohibited by the Fourth Amendment. *Id.* The Court reasoned that an individual in an automobile traveling on public highways and roads has no reasonable expectation of privacy. *Id.*

66. *See Kyllo v. U.S.*, 533 U.S. 27 (2001).

67. *See Katz*, 389 U.S. at 352, 355. Other well known Supreme Court cases on point are *Dow Chem. Co. v. U.S.*, 476 U.S. 227 (1986), and *Cal. v Ciraolo*, 476 U.S. 207 (1986), which also apply the rules from *Katz*. In *Dow Chem. Co.*, the Environmental Protection Agency requested permission from Dow Chemicals to investigate the corporation's facility onsite, but the request was denied. 476 U.S. at 229. Thereafter, the Environmental Protection Agency, without a warrant, hired a commercial aerial photographer to photograph the plant from varying altitude levels in lawful airspace. *Dow Chem. Co.*, 476 U.S. 230. When the Corporation learned of the photographs, it filed suit claiming a Fourth Amendment rights violation. *Id.* The Court held that there was not a violation of privacy rights because the open spaces of the corporation's facility are analogous to an open field, where an individual cannot reasonably and legitimately demand privacy, even if in regard to private property. *Dow Chem. Co.*, 476 U.S. 235. Moreover, the Court held that enhancement of natural vision does not give rise to Constitutional issues. *Dow Chem. Co.*, 467 U.S. 238. In other words, the use of any technology, which improves human eyesight, does not violate privacy rights. *Id.* Aerial photography was also utilized in *Ciraolo*, but in this case the search was for marijuana plants. 476 U.S. at 209. After the police received an anonymous lead that Mr. Ciraolo was growing marijuana in his backyard, they obtained a private plane to get an aerial view of the property. *Id.* Thereafter, the officers could see, and also photograph, the eight to ten foot tall marijuana plants in Ciraolo's backyard. *Id.* With this evidence, a warrant was obtained and the plants seized. *Ciraolo*, 476 U.S. 210. Mr. Ciraolo met the first step in the *Katz* test by expressing his subjective intent to maintain the privacy of his marijuana plants with the ten-foot fence around his property, but this phase of the test was not contested. *Ciraolo*, 467 U.S. 211. This court defined the second step of *Katz* as a question of legitimacy based on whether the intrusion is upon societal values that

growing marijuana in his home and used Thermal Imagers to detect high-intensity lamps that are required to grow the plant indoors.[68] Thermal-imaging technology identifies infrared radiation released by most objects, but is invisible to the human eye.[69]

Based on English law,[70] courts have held that a visual observation is not a search because the eyes cannot be guilty of trespass.[71] However, the surveillance in *Kyllo* was accomplished by a sophisticated technology much stronger than the naked eye.[72] The information gained by the government through sense-enhancing technology could not otherwise have been obtained without physically entering the home, which is constitutionally protected.[73] Therefore, the Court held that a search occurs when an instrument that is not available to the public is used to investigate a home, which, without the technology, would normally require physical entrance to obtain such information.[74]

---

the Fourth Amendment protects. *Ciraolo,* 467 U.S. 212. The court then addressed the second step as related to this particular case, which is whether society will recognize the expectation of privacy as reasonable. *Id.* The Supreme Court held that Mr. Ciraolo's expectation of privacy regarding his backyard was unreasonable and society will not honor that expectation. *Ciraolo,* 467 U.S. 213. The reasoning for the Court's decision is that the officers' observations were from public navigable airspace, they were able to recognize the marijuana plants with their naked eyes, and it was unobtrusive. *Id.*

68. *See Kyllo,* 533 U.S. 30.

69. *See Kyllo,* 533 U.S. 30. The issue before the court was whether the use of such a technological device directed at a private residence for the purpose of finding relative amounts of heat from inside the home is a search within the meaning of the Fourth Amendment. *Kyllo,* 533 U.S. 29-30.

70. *See Kyllo,* 533 U.S. 32 (quoting *Entick v. Carrington*, 95 Eng. Rep. 807 (K.B. 1765)).

71. *See Kyllo*, 533 U.S. 32; *Ciraolo*, 476 U.S. 213 (illustrating that Fourth Amendment privacy rights do not demand that law enforcement officials cover their eyes as they pass a private residence).

72. *See Kyllo,* 533 U.S. 34.

73. *See Kyllo,* 533 U.S. 41; *U.S. v. Santana*, 427 U.S. 38 (1976). The defendant in *Santana* was standing in the threshold of her home when the police identified themselves and then she retreated into the confines of her residence. 427 U.S. 40. The Court held that a person could not evade an arrest, which began in a public place, by retreating into a private home. *Santana,* 427 U.S. 43.

74. *See Kyllo*, 533 U.S. 34. In other words, a warrant must be obtained if law enforcement plans to utilize a device that is unavailable to the public because the search would be "presumptively unreasonable without a warrant." *Kyllo,* 533 U.S. 39. Comparatively, the Court in *Ciraolo* held that a person does not maintain privacy in his backyard even if a fence is present, because anyone with the capability of flying a plane over this property could observe what was located within the fence. 476 U.S. at 213. Chartering a private plane or getting a pilot's license are opportunities available to all people interested. *See* Air Charter Team, *Services* §§ 1, 4 <http://www.aircharterteam.com/specialty.htm> (accessed Nov. 28, 2001) (marketing the different types of flights offered by the respective company, such as VIP and Executive Charters and Cargo); Be A Pilot, *Learning to Fly* § 1 <http://www.beapilot.com/brochure/must.html> (accessed Nov. 28, 2001) (listing requirements for becoming a pilot, which are must be sixteen years old, speak English, and pass a medical

C. Arguments on Either Side of the Privacy Issue

Privacy advocates believe that surveillance technologies tread on the privacy rights of ordinary citizens.[75] Arguments against the use of facial-recognition technology are based on an individual's constitutional right to be free from unreasonable searches.[76] Specifically, they are concerned about storing identities in databases and the high probability for the technology to be used for racial profiling and unwarranted monitoring of political activists.[77]

On the other hand, safety and security of common every day activities, such as working and traveling, is of the utmost importance to the general public considering the recent terrorists attacks directed at the innocent citizens of this country.[78] Facial-recognition technology is an

---

examination). Therefore, by applying *Kyllo* to *Ciraolo*, a warrant would not be necessary because the technology was available to the general public. *Kyllo*, 533 U.S. 33.

75. Sullivan, *supra* n. 22, at ¶ 13; *contra* Am. Civ. Liberties Union Freedom Network, *Firms Defends "Snooper Bowl" Technology* ¶ 7 <http://www.aclu.org/news/2001/w030901a.html> (Mar. 9, 2001). The CEO of Viisage, Thomas Colatosti, argues that facial-recognition technology actually improves an individual's privacy by making it more arduous, and potentially impossible, to access personal information. *Id.* He commented that the technology could be implemented to prevent the theft of identities and secure financial accounts. *Id.*

76. In *Griswold v. Conn.*, executives and directors of the Planned Parenthood League were convicted of violating a Connecticut statute, which made the use of contraceptives a criminal offense. 381 U.S. 479, 480 (1965). The defendants were charged with instructing and giving advice to married couples about ways to avoid pregnancy. *Id.* The Supreme Court held that the right of marital privacy was violated by the Connecticut statute. *Griswold,* 381 U.S. 485. This relationship was within the "zone of privacy," which is formed by Constitutional guarantees. *Griswold,* 381 U.S. 486. These Constitutional guarantees are the First Amendment's right of association, the Third Amendment's preclusion of quartering soldiers during peacetime, the Fourth Amendment's protection from unreasonable searches and seizures, the Fifth Amendment's self-incrimination clause, and the Ninth Amendment's prohibition on construing rights in order to deny other rights held by people. *Griswold,* 381 U.S. 485.

77. *See* Casino Mag., *supra* n. 8, at ¶ 8.

78. Support for facial-recognition technology by society in general has increased dramatically since the tragic attack on the World Trade Center and the Pentagon. *See* Kuykendall, *supra* n. 30, at ¶ 6. Evidence of such increase is found in the financial markets where stock prices of several of the major Biometrics corporations, such as Viisage, Visionics, and Identix, increased by more than a hundred percent on the trading day following the tragedy in New York and Washington, D.C. *Id.* Analyst prospect the reason for the increase is due to a growing acknowledgment that these technologies offer a solution to our nation's security dilemma. *Id.* Citizens have unfortunately realized that we are not alone in this world and must devise better ways of protecting ourselves by preventing future attacks. *Id.* Another indicator of public opinion is a recent Harris Poll, which surveyed 1012 adults. Frank Thorsberg, *PC World Poll Highlights Privacy Concerns* § 6 <http://www.cnn.com/2001/TECH/industry/10/08/privacy.poll.idg/index.html> (accessed Oct. 8, 2001). This poll determined that 86 percent of those asked supported the use of facial-recognition technology. *Id.* Other results of the poll indicated eighty-one percent of those surveyed advocated for more monitoring of banking and credit card transactions and sixty-

effective and efficient method of securing our country's corporate and government buildings, airports, and other facilities by tracking known criminals and terrorists. This technology is necessary to prevent further terrorist attacks and it should not be dismissed because of a mere potential for abuse when precautions can be implemented. Banning this technology for its negative potential is like banning the use of automobiles because there is a chance they could be involved in accidents. The advantages of using this technology are far greater than the possibility that it could be misused.

Both of the leading companies for facial-recognition software have implemented their own guidelines in marketing their respective products.[79] Visionics limits what type of information may be accumulated and saved in the facial-recognition database.[80] Furthermore, it monitors its customers' use of the software to ensure it is not manipulated to capture and store identities of common citizens.[81] Also, Viisage's corporate policy is even more strenuous as it will not enter into an agreement with an entity if it believes the particular purpose is or has potential to be invasive.[82] As positive as it appears that the Biometrics industry is regulating itself, advocates of both privacy and facial-recognition technology believe there are too many dangers associated with these self-imposed guidelines, such as fraud and other illegal use of the technology.

Both the biometrics industry and advocates for privacy agree that legislation is required to prevent misuse of the technology by governmental agencies, corporations, or private citizens.[83] The Biometrics industry

---

eight percent supported a national identification system. *Id.* In another poll taken by Business Week, more than sixty percent of the 1334 respondents surveyed said they would submit to a face scanning at a transportation hub or public event. *Id.* Other results from the Business Week survey are sixty percent of those individuals polled would accept a national identification card and over fifty percent supported governmental scanning of email messages and telephone conversations. *Id.* Additionally, about fifty percent of the respondents approved more wiretapping and e-mail surveillance by the government. *Id.* On October 25, 2001, the Senate approved a broad legislation on anti-terrorism by a vote of ninety-eight to one, which has the effect of increasing the scope of the government's authorization to conduct electronic surveillance. Adam Clymer, *Senate Clears Anti-Terror Bill for Bush's Signature* ¶¶ 1, 3 <http://www.nytimes.com/2001/10/25/politics/26CONGRE.html> (accessed Oct. 25, 2001).

79. Sullivan, *supra* n. 22, at ¶ 2.

80. *Id.*

81. *Id.*

82. *Id.*

83. *See id.*; George, *supra* n. 12, at ¶ 13. In light of the September 11th events, the Supreme Court Justices are regarding the legal implications of security measures to prevent further terrorist attacks on U.S. soil, though the Court's docket does not reflect that consideration. Linda Greenhouse, *Supreme Court Roundup: In a New Climate of Unity, Divisive Issues Remain* ¶ 3 <http://www.nytimes.com/2001/10/01/national/01SCOT.html> (accessed Oct. 1, 2001). Justice Sandra Day O'Connor was quoted as saying the attacks of September 11th have "already altered our way of life, and it will cause us to re-examine

acknowledges the need for specific guidelines through legislation and it implores Congress to look at the "harsh new realities"[84] this country must now face.[85] Furthermore, it urges Congress to utilize the aggressive technology based responses that such situations require.[86] Conversely, privacy advocates argue for a narrow implementation of the technology to prevent a loss of autonomy and, specifically, racial profiling and voyeurism.[87] This Comment will outline objectives for new legislation that will protect privacy interest while offering the citizens of this country revolutionary technology based methods of security and protection.

III. ANALYSIS

This section of the Comment will prove that facial-recognition technology does not violate an individual's right to privacy because there are no reasonable expectations of privacy in public places.[88] Furthermore, the system's databases will only contain the identities of known criminals and terrorists[89] and facial-recognition technology is analogous to already utilized law enforcement procedures. Lastly, the Comment outlines potential legislation on this technology to ensure rights to privacy are not violated.

---

some of our laws pertaining to criminal surveillance, wiretapping, immigration and so on." *Id.*

84. George, *supra* n. 12, at ¶ 13.

85. *Id.*

86. *Id.*

87. Am. Civ. Liberties Union Freedom Network, *supra* n. 75, at ¶ 15. An example of the privacy sector's shift to better acknowledging a need for more security is the resignation of a very well respected privacy expert, Richard Smith, from the Privacy Foundation. Stefanie Olsen, *Privacy Expert Resigns To Focus On Security* ¶ 1 <http://news.com.com/2102-1023-275250.html> (accessed Oct. 31, 2001). Smith commented that his reason for leaving were that the government is going to spend ten billion dollars on security measures and he wants to ensure that the money going towards technologies is spent properly. *Id.* at ¶ 5. He is planning on working as a consultant with the government and other organizations to make the best possible determinations on what security systems are appropriate for which situations. *Id.* at ¶ 4. Many other privacy advocates have shifted their priorities after the World Trade Center and the Pentagon attacks from defending civil liberties to developing better security measures for our country. *Id.* at ¶ 7. This shift is due to the larger change of the public's perception about what this nation's priorities should be at this point. *Id.* at ¶ 6. In fact, most people now believe that privacy should be placed in the background until we can feel secure again. *Id.* at ¶ 7.

88. *Katz*, 389 U.S. at 351.

89. Access Control & Security Systems Integration, *Industry Leaders Call for Federal Legislation on Facial Recognition* ¶ 10 (Sept. 25, 2001) (available in LEXIS, News library, Individual Publications file).

A. PRIVACY

1. *Based on the Rules from Katz and Kyllo, Facial-Recognition Technology Does Not Invade Privacy*

a) No Legitimate Expectation of Privacy in Public Places

No individual can reasonably expect to maintain privacy in a public forum.[90] Facial-recognition technology will be implemented in public places, such corporate and government buildings, busy sidewalks, sports events and airports. These public places are analogous to open fields. Courts have held there can be no legitimate and reasonable expectation of privacy in an open field.[91] Therefore, the use of facial-recognition technology, when used in public locations similar to those mentioned above, does not violate the Fourth Amendment because there cannot be a reasonable expectation of privacy in public places.[92]

The use of facial-recognition technology is distinguishable from the technology used in *Katz*, which held a warrant was required for the wiretapping to be a constitutional search.[93] Facial-recognition is based on visual surveillance, which has long been held not to fall within the scope of the constitution, rather than a wiretap.[94] Therefore, facial-recognition technology does not violate privacy rights.

The use of facial-recognition technology can also be contrasted from the thermal image technology used in *Kyllo*.[95] First, facial-recognition technology does not intrude into the interior of a private residence, but is utilized only when the suspect reveals himself to the public. In fact, it is extremely non-intrusive because the software can scan a crowd without requiring active participation from an individual.[96]

Secondly, video surveillance is not a search regulated by the Fourth Amendment because it is capturing exactly what the naked eye be-

90. *See id.*; *Dow Chem. Co.*, 476 U.S. 227; *Ciraolo*, 476 U.S. 213. An example of a location where a reasonable expectation of privacy would be found is within an individual's home. *Santana*, 427 U.S. 42. Furthermore, *Knotts* held that there is no reasonable expectation of privacy on public highways. 460 U.S. 276. Public highways are analogous to public forums, such as sidewalks and busy corporate buildings, because both leave people exposed to the views of others.

91. *See Dow Chem. Co.*, 476 U.S. 239.

92. *See Katz*, 389 U.S. 351.

93. *See Katz*, 389 U.S. 359.

94. *See Dow Chem. Co.*, 476 U.S. 234-35. The Supreme Court has held that visual surveillance is not a search. *Id.* Law enforcement officials are not required to cover their eyes as they pass a private residence in order to remain within their constitutional duty. *Ciraolo*, 476 U.S. 213.

95. *See Kyllo*, 533 U.S. 29.

96. Mary Kirby, *Biometrics Firms Expect Big Business as Security Clamps Down*, Air Transport Intelligence ¶ 5 (Sept. 28, 2001) (available in LEXIS, News library, Individual Publications file); Rutherford, *supra* n. 23, at ¶ 6.

holds.[97] The technology used in *Kyllo* did not enhance a human's natural vision, but detected infrared radiation, which is invisible to the naked eye without advanced electronic assistance. The reasoning behind this rule is that "[w]hat a person knowingly exposes to the public. . . is not a subject of Fourth Amendment protection."[98] The purpose of facial-recognition technology is not for identifying individuals within their homes. This type of usage is illogical. If law enforcement need to implement facial-recognition technology on a private residence, the identity of the individual living in the home would already have been ascertained.[99] As a result, facial-recognition technology would not be necessary and, therefore, the sanctity of the home will be protected.

Furthermore, facial-recognition technology is constitutional under the rule established in *Kyllo*.[100] *Kyllo* holds that a warrant is necessary if the government employs a device not readily available to the general public to gain information about a private residence that would normally require physical entrance.[101] Facial-recognition software is available to the general public because it can be purchased at local computer or electronics stores for only a hundred dollars.[102] As a result, the implementation of facial-recognition technology conforms to the rule in *Kyllo*.

b) Expectations of Privacy from the Use of Facial-Recognition Technology are Not Recognized as Reasonable by Society

Society will not recognize an expectation of privacy from the use of facial-recognition technology as reasonable. This is the result of our society's awareness of the world outside the United States' borders.[103] Due

97. *See Kee v. City of Rowlett, Tex.*, 1999 U.S. Dist. LEXIS 7938 (N.D. Tex. Jan. 27, 1999). In deciding if a reasonable expectation of privacy is present, the court looks at (1) whether the person has an interest in the place searched, (2) if the individual has a right to exclude people from the location, (3) if the person has displayed a subjective expectation of privacy, (4) whether the individual took steps to protect privacy, and (5) if the individual was lawfully on the premises. *Id. at* **5-6. The Court in *Kee* held that the warrantless video surveillance of an individual during a prayer service in a graveyard was not an invasion of his Fourth Amendment right to privacy. *Id.*

98. *See Katz*, 389 U.S. 351; *St. of Haw. v. Augafa*, 92 Haw. 454 (Inter. Ct. of App. Ha. Dec. 22, 1999) (holding that an observation by a law enforcement officer of activities in open view is not within the scope of reasonable expectations of privacy and also is not protected by Constitution).

99. *See* Milligan, *supra* n. 3, at 318. Law enforcement could determine the identity of the suspected individual by asking neighbors, investigating the deed on the home, and crossing the address with the Department of Motor Vehicle. *Id.*

100. *Kyllo*, 533 U.S. 39.

101. *See id.*

102. Milligan, *supra* n. 3, at 304.

103. This country is in a state of heightened alert as a result of the attacks against innocent civilians on September 11, 2001. *See generally* Patrick Tyler and Elaine Sciolino, *A Nation Challenged: As U.N. Meet, Bin Laden Tape Sets Off Alarms* <http://

to the current events in this country, our society is more prepared than ever to take whatever means are necessary to protect us and our families. This issue relates to the second prong of the expectation of privacy test set forth in *Katz,* which is whether society will recognize the particular expectation of privacy held by an individual as reasonable.[104]

The use of facial-recognition technology will not be considered by society as a violation of the Fourth Amendment because there are no reasonable expectations of privacy in public places and facial-recognition technology is used in public places.[105] The benefits of implementing facial-recognition technology are far more important than benefits of rights to privacy in public places. Therefore, the people of this country are not willing to protect such privacy at the price of risking their safety. This country is embroiled in a new war where information intelligence is essential to our success.[106] Society recognizes the need for monitoring public locations in order to locate criminals and known terrorists and promotes facial-recognition technology for its ability carry out that responsibility.

2. *Databases Used by Facial-Recognition Technology Only Contain Identities of Known Criminals and Terrorists*

Opponents of facial-recognition software are fearful of the technology eroding personal freedoms, such as autonomy, which are so precious to the American lifestyle.[107] Specifically, they fear this technology will be used to monitor and track innocent citizens and to discriminate racially and politically.[108] Moreover, apprehension that facial-recognition technology has a high propensity to be abused fuels the already existing concerns that rights to privacy will be eroded with

---

query.nytimes.com/search/article page.html?res=9402EFD61638F93AA35752C1A9679C8B63> (accessed Nov. 9, 2001) (quoting Osama Bin Laden as calling the terrorist attacks "great strikes that hit the United States in its most important locations"). It is unfathomable that in a modern and advanced society as ours that a few men with crude weapons could cause so much devastation. *Id.* After the attacks, the public began to question what measures we could take to better protect ourselves from future assaults. *See* Thorsberg, *supra* n. 78, at § 6.

104. *Katz,* 389 U.S 352, 355; *Ciraolo,* 476 U.S. 211. This phase of the test relies on whether the invasion by the government infringes upon values that are not only personal, but also societal and privileged to Fourth Amendment protection. *Ciraolo,* 476 U.S. 212.

105. *See id.*

106. With future legislation, law enforcement agencies will become better at sharing information with other agencies through the implementation of databases, like those used by facial-recognition software. *See* Casino Mag., *supra* n. 8, at ¶ 30.

107. Kirby, *supra* n. 96, at ¶¶ 12-13; Rutherford, *supra* n. 23, at ¶ 8 (explaining that advocates for privacy call scanning an individual's faces a "covert invasion of privacy").

108. Casino Mag., *supra* n. 8, at ¶ 8.

its implementation.[109]

Contrary to these views, facial-recognition technology only identifies criminals who are filed in the system's databases and does not automatically store images of ordinary citizens who pass by its line of sight.[110] Some facial-recognition products can only be used to verify an individual's identity for access to an organization's resources.[111] In particular, one of the facial-recognition technology corporations has stated that its system discards facial identification information after a short period of time.[112] Because the software does not store the identities of non-criminals, there is no way for those individuals to be monitored or to be racially or politically profiled. Biometric technology was designed to locate and identify criminals, not innocent people.[113]

3. *Comparing Facial-Recognition Technology to Existing Criminal Procedures*

The foundation of facial-recognition technology is similar to a police officer standing in a crowd with a stack of mug shots and comparing them to people who walk past him.[114] The technology is enhancing the

---

109. Sullivan, *supra* n. 22, at § 2. Advocates of privacy rights are also concerned that facial-recognition software will be rushed into implementation prior to adequately testing its abilities and functionality. *Id.* at § 1.

110. Access Control & Security Systems Integration, *supra* n. 89, at ¶ 10. The facial-recognition databases obtain criminal identities from local, regional, and international sources of criminal profiles and aliases. PR Newswire, *supra* n. 22, at ¶ 5. Also, databases link with international and national agency jurisdictions to identify terrorists and their accomplices. Kirby, *supra* n. 96, at ¶ 6.

111. Dave Kearns, *Biometrics and Privacy* ¶ 2 <http://www.nwfusion.com/ newsletter/ dir/2000/0605dir2.html> (accessed May 7, 2000).

112. Steve Gold, *U.K. Bookstore Kills Customer Face-Recognition Project*, Newsbytes ¶ 12 (Aug. 28, 2001) (available in LEXIS, News library, Individual Publications file). Images are usually discarded thirty days after it has been captured. *Id.* Visionics also stated that the facial-recognition technology only indicates how many times a certain face has been observed by the system, not that certain racial profiles are followed more closely than others. *Id.*

113. Kuykendall, *supra* n. 30, at ¶ 7; George, *supra* n. 12, at ¶ 5. It is not likely that law enforcement officials would have fingerprint information on terrorists groups, but it is more reasonable that they would have their pictures. *Id.*

114. Brahm Rosenweig, *Smile for the Camera: Someone Could Be Watching You Right Now* ¶ 7 < http://exn.ca/Stories/2000/06/07/52.asp> (accessed June 7, 2000). Facial-recognition software is a real time version of a police officer looking through pictures for a match. This idea is based on the principal that facial-recognition technology imitates the human capability of recognizing another person. *Id.* Similarly, *Costin* held that the use of electronic surveillance is the same as a police officer undercover in a stakeout observing some action or movement with his own eye. 168 Vt. 182. It makes no difference that the image seen with the naked eye is recorded on film rather than in one's own memory. *Id.*

basic human skill of matching faces to identities in pictures.[115] In fact, a computerized method of matching faces has a high probability of being more accurate than the law enforcement officer's own eyesight and judgment.[116] Facial-recognition technology does not violate privacy rights because it is merely making a procedure currently used by law enforcement more efficient.

Facial-recognition technology is also similar to fingerprinting, which has been used to identify perpetrators of crimes for over a century.[117] Fingerprinting compares prints that have been pulled from objects with a database of other prints. This is the same basic procedure used in facial-recognition technology, which matches faces to identities within its own database.[118] Fingerprinting is a law enforcement procedure that has been authorized by statutes and been used for a hundred years.[119] Facial-recognition technology does not violate privacy rights because it employs the same procedures as fingerprinting. If fingerprinting does not violate the constitution, then neither should facial-recognition technology.

B. Proposals for Legislation on Facial-Recognition Technology

Along with privacy advocates, the Biometrics industry is also calling for legislation on the use of sense-enhancing technology.[120] There are two general issues that must be addressed in regards to legislation on

115. Facial-recognition technology is similar to the use of drug-sniffing dogs. The Court has held that a drug dog's indication of the presence of narcotics is not a search under the Fourth Amendment. *U.S. v. Place*, 462 U.S. 696, 707 (1983). Following the logic from *Place*, the use of facial-recognition technology, which only identifies illegal activity, such as a known terrorist in an airport, would also not be classified as a search and, thus, constitutional. *Id.* Facial-recognition software is "blind as a bat" if it is not linked with a database of known identities. Rutherford, *supra* n. 23, at ¶ 12. Frances Zelazney, the director of corporate communications for Visionics, stated that the purpose of the system is not to add individuals to the file. *Id.* Because innocent individuals are not added or monitored, privacy rights are not being violated. *Id.*

116. Chachere, *supra* n. 7, at § 4.

117. Pimentel, *supra* n. 9, at ¶ 18. The major difference between fingerprinting and facial-recognition technology is the need for active participation from an individual in the fingerprinting process. Rutherford, *supra* n. 23, at ¶ 7.

118. After the police have lawfully detained a person, they must submit to fingerprinting as a common practice for obtaining accurate identification. *U.S. v. Krapf*, 285 F.2d 647, 650 (3d. Cir. 1960). Fingerprint databases, similar to facial-recognition technology, are obtained from suspected or convicted perpetrators of crimes. *Id.*

119. *See* 28 U.S.C.S. § 534(a)(1) (2000). The Attorney General has the responsibility to gather, categorize, and maintain identifications or any information that would assist in identifying persons. *Id.*

120. Sullivan, *supra* n. 22, at § 2. The CEO of Visionics Inc., Dr. Atick, has requested that facial-recognition be of utmost public policy and has called for federal legislation concerning the Biometrics industry's guidelines and Closed-Circuit Television (CCTV). Access Control & Security Systems, *supra* n. 89, at ¶ 1.

this subject, scope and regulation. The solution to the debate between privacy and the need for adequate and effective security measures can be resolved with appropriate legislation.[121]

1. *Scope*

It is imperative that legislation defines the scope broadly enough to ensure the technology can be used effectively, but not so broad as to trample upon reasonable expectations of privacy. In order to prevent invasions of privacy, Congress should reiterate that warrantless sense enhancing searches should only be implemented in public places or open spaces, where expectations of privacy are minimal. Requiring law enforcement officers to obtain warrants for searches not conducted in public places protects the privacy of an individual not exposed to public view.[122] Moreover, visual surveillance systems, which operate with facial-recognition software, should be openly exposed to the public's view and not secretly placed.

Furthermore, legislation on this issue should disallow stockpiling identifications of innocent individuals who, by chance, cross the camera's field of vision. There is no present purpose for these systems to automatically retain such information and privacy advocate's fears will be substantially subsided. However, legislation should not prevent companies from storing identities in databases as long as permission is received from each individual.[123] Companies, with permission from the identity holder, should be limited in reselling images of individuals it captures during surveillance, such as to direct marketing firms who then inundate the consumer with advertisements. Companies could direct market to only those individuals who have pre-approved the disbursement of their identities for that purpose.

---

121. It is naïve to assume that advocates will ever be able to find an absolute equal footing between these two important social values. Olsen, *supra* n. 87, at ¶ 1. However, it does appear that the respective parties acknowledge the attributes of the opposing side and the need for both privacy and security. *Id.* at ¶¶ 4, 5. As a result, they will be more likely to bend or concede on certain issues for a fast resolution. *Id.*

122. The American Bar Association has developed standards, which analogize electronic surveillance of private places with wiretapping. Milligan, *supra* n. 3, at 323. Facial-recognition technology would be allowed if the reasonable result would be a legitimate law enforcement objective, approved by a "politically accountable" public official, and the public gets a chance to comment. *Id.* When for deterrence purposes, the proposition is that the public should be notified for an opportunity to comment on the usage. *Id.*

123. *See* Lavonne Kuykendall, *Grocer Seeks Boost Through Biometrics*, Am. Banker ¶¶ 2, 13 (May 7, 2002) (available in LEXIS, News Library, Individual Publication file) (discussing grocers use of biometrics as method of payment for goods purchased and potential loyalty programs to be incorporated into the technology).

2. *Regulation*

Until legislation on the use of sense-enhancing technology is passed, the Biometrics industry will be utilizing its own self-imposed guidelines to prevent abuse of the technology's capabilities.[124] However, fundamental problems arise when an industry participates in self-regulation, such as manipulation of guidelines to increase economic gain and fraudulent behavior. As a result, how the technology will be exercised and who will monitor its use must be decided by Congress.[125]

Facial-recognition technology, along with all the other divisions of Biometrics, is best left to the federal government to regulate. Specifically, regulation should be left under the control of Homeland Security. One controlling body will ensure the defined scope of the technology is protected through uniformity of legislation. The alternative action leaves the decision in the hands of the individual States to determine how to regulate. However, many varying rules on the technology's application create a greater probability that privacy will be invaded unreasonably. One regulatory body creates a more efficient means to handle issues that may arise from the use of the technology because responses will be consistent and standardized.

Homeland Security will be the police force behind ensuring that the laws on facial-recognition technology are followed. Congress should incorporate heavy monetary penalties against parties who do not use the software according to legislative guidelines. Additionally, pecuniary penalties should be assessed against Biometric corporations who knowingly sell their product to organization who will misuse the technology.

Privacy advocates argue that facial-recognition technology is not cost effective because additional security staff is required to run the software adequately. Contrary to this argument, the implementation of facial-recognition technology will not create the need to spend capital on more security personnel. Instead, it will make the duties of existing personnel more efficient. The reason for the added efficiency is that security staff will spend less time monitoring the crowds because the software will handle that responsibility. Consequently, there will not be a need for more security personnel to handle the technology because the existing staff will have more time to respond to suspicious activity or people.

The result of this regulation impacts both law enforcement and citizens positively by creating a broad scope for the implementation of facial-recognition technology with a focus on safeguarding privacy. Law

124. Sullivan, *supra* n. 22, at § 2. Visionics Corp. will not market its software in certain circumstances if the company feels that the monitoring would be invasive. *Id.*

125. *See* 18 U.S.C. §§ 2510-21 (1994); Burrows, *supra* n. 60, at 1096. Congress does not appear to be willing to pass a law that prohibits the video surveillance of individuals. *Id.*

enforcement officials have a powerful and effective tool in their arsenal to catch known criminals and terrorists. Furthermore, citizens can feel more secure knowing that the best and most current technology is being used to protect them.

IV. CONCLUSION

Now is not the time to ponder, but to act. This country has the ability and technology necessary to prevent attacks on this country from foreign enemies, such as the attack on September 11, and from common crimes perpetrated on our streets, like robbery and sexual assault. Aside from private residences, facial-recognition technology must be implemented wherever suspected terrorists and criminals can cause harm. This country can no longer sit idly by and believe that terrorist attacks cannot happen on our own soil. When we are aware of our enemy's identity, all reasonable steps must be taken in order to prevent that person from carrying out his evil intentions.

Facial-recognition technology is the perfect weapon to protect this country from such evil elements. It is non-invasive and requires little to no active participation from the public. The software's accuracy rate, coupled with its noninvasive character, makes it the most effective tool for scanning large crowds or open and busy areas in search for known terrorists and criminals. Furthermore, databases used by the technology are compiled only of known terrorists and criminals. Consequently, innocent citizen cannot be tracked and monitored unless they have given their permission.

Facial-recognition technology does not violate privacy rights because visual surveillance is not a constitutional issue. The technology, when used in public places, does not violate the Constitution because the Fourth Amendment because reasonable expectations of privacy do not exist in public places and society will not constitutionally protect that expectation by qualifying it as legitimate. Furthermore, the government does not have to shield its eyes from activities occurring within its line of vision. Facial-recognition technology only improves the procedure of comparing faces to mugshots and does not enhance natural human vision.

These are changing times, which is evident by society's shift of its priorities from protecting our privacy rights to the need for more security for our nation's safety. Society is not willing to grant freedom from facial-recognition technology by allowing individuals to have reasonable expectations of privacy in public places. Facial-recognition technology is

the first major step to the larger solution of ending terrorist attacks and decreasing criminal activity.

Susan McCoy†

† Susan McCoy will complete her Juris Doctor in June 2003 and will specialize in transactional law. The author wishes to thank her family and friends for their patience and support throughout law school. Furthermore, she wishes to extend her gratitude to the Journal for their assistance with this Comment.