UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 3
Issue 1 *Fall 2001*

Article 9

10-1-2001

Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveilance Systems

Kanya A. Bennett

Comment: Can Facial Recognition Technology Be Used To Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems

Kanya A. Bennett[1]

I. Introduction

The images of the September 11, 2001 tragedy are still vivid for most Americans. In light of these events, many citizens want to know how to prevent terrorist acts from happening again. Most agree that the American way of life will forever be changed. An expectation to travel around the country at a moment's notice is no longer reasonable, nor are Americans as likely to demand living our lives with little or no interference from the government. While most Americans seemingly expect and are willing to sacrifice some freedoms for assurance that we can live our lives in safety, many wonder just how much we will have to sacrifice for such assurances.

Because Americans live in one of the most technologically advanced societies, our lives have already been monitored and our freedoms constrained by highly intrusive means. Employers can legally monitor their employees' e-mails, and automobile drivers can be issued traffic tickets with the use of video cameras attached to stoplights. This comment will focus on one of the most intrusive means that recent technological advancements will now allow to be imposed upon us in the name of combating crime and ensuring safety: facial recognition.

---

[1] J.D. Candidate 2002, University of North Carolina School of Law; B.S., University of Illinois, Champaign-Urbana.

Facial recognition is part of a larger category of technologies called biometrics that uses biological information, such as iris scans and handprints, to confirm identity.[2] The use of facial recognition software in conjunction with public video surveillance ("facial recognition surveillance") is quickly emerging as a means of tracking down criminals and other wanted individuals. In light of the September 11th tragedy, inquiries into how this technology can be used to prevent future attacks of this kind are now being explored with great urgency. Countering these inquiries are concerns that this form of electronic surveillance may be so intrusive that it violates our constitutional rights.

This Comment sets out to explore the constitutionality of facial recognition surveillance in the context of the Fourth Amendment. The evolution of this type of electronic surveillance will be examined in Part II of this article. Part III of this article will concentrate on how this technology works and will focus on its use in the first United States city to implement such surveillance. Part IV will discuss this type of surveillance and possible Fourth Amendment implications. The use of facial recognition technology in response to a national security interest, such as that created by the September 11th tragedy, will also be discussed in Part IV. Part V will conclude the Comment with a discussion of possible safeguards that should be put in place for this technology to operate effectively, whether use of the technology is in fact constitutional or only warrants use in certain situations.

---

[2] Emelie Rutherford, *Facial-Recognition Tech Has People Pegged* (July 17, 2001), *at* http://cnn.com/2001/TECH/ptech/07/17/face.time.idg (on file with the North Carolina Journal of Law & Technology).

II. Evolution of Facial Recognition Technology in the United States

In the early 1960s, public video surveillance was introduced into the private sector and utilized primarily by banks.[3] By the next decade, use of this surveillance was widespread and found in places such as hospitals and convenience stores.[4] However, use of this technology was limited because remote active monitoring of video was relatively unavailable, and the quality of film and cameras often resulted in blurry images.[5] Starting in the mid-1980s, improvements began to be made with video technology and these problems were minimized.[6] These new advancements included things such as zoom lenses and digital technology.[7] This allowed video cameras to collect distinct, vivid images without much lighting.[8] With the expansion of video capabilities came experimentation with this form of technology and biometrics. Practical applications merging biometrics technology, particularly facial recognition, with video technology were first sought after by the United States government as a possible means of ensuring national security.[9]

---

[3] MARCUS NIETO, PUBLIC VIDEO SURVEILLANCE: IS IT AN EFFECTIVE CRIME PREVENTION TOOL? (June 1997), *available at* http://www.library.ca.gov/CRB/97/05/ (on file with the North Carolina Journal of Law & Technology).

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

[9] John D. Woodard, *Biometric Scanning, Law & Policy: Identifying the Concerns--Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 109 (1997).

The United States Department of Defense has funded university scientists' work on facial recognition technology for over a decade.[10] Department of Defense officials have been focused on perfecting this technology to better spot criminals at our country's borders.[11] Likewise, private companies determined that this technology could combat crime within the country's borders and began marketing use of this technology in the mid-1990s.[12]

A few companies have developed facial recognition software to be used in conjunction with video surveillance cameras; the most well-known of these is Visionics Corporation of Jersey City, New Jersey. In addition to marketing its product as a high-tech, identity recognition device that can be used to combat crime, Visionics Corp. also describes its facial recognition system as an efficient means to verify employee and student identity.[13] In order to understand the vast capabilities of facial recognition surveillance, it is necessary to have a basic understanding of how this technology works.

[10] Rutherford, *supra* note 2.
[11] *Id.*
[12] *Id.*
[13] Visionics Corp. website, *at* http://www.visionics.com/faceit/whatis.html (last visited September 21, 2001) (on file with the North Carolina Journal of Law & Technology) (providing a description of FaceIt applications and uses).

III. How Facial Recognition Technology Works and Its Use in the United States

A. How Facial Recognition Technology Works

The use of facial recognition software with video surveillance is a complex technological process. In marketing its software FaceIt, Visionics Corp. has offered a layperson's description of how its product works. Video cameras are used to scan an area.[14] Faces within a 35-degree angle of the camera can be extracted from the people in the monitored area.[15] It takes only a split second for the camera to identify a face from among the other images it is monitoring.[16] The software then measures between fourteen and twenty-two of the approximately eighty nodal points that make up an individual's face.[17] Nodal points are those facial features that make each face unique.[18] Nodal points include such characteristics as depth of eye sockets, distance between eyes, and width of nose.[19]

Once these points have been identified, the nodal point measurements are turned into a comprehensive numerical code, which is called a faceprint.[20] Millions of faceprints can be compared to the database of stored faceprints in a minute.[21]

---

[14] Kevin Bonsor, *How Facial Recognition Works, at* http://www.howstuffworks.com/facial-recognition.htm (last visited Oct. 8. 2001) (on file with the North Carolina Journal of Law & Technology).
[15] *Id.*
[16] *Id.*
[17] Rutherford, *supra* note 2.
[18] Bonsor, *supra* note 15.
[19] *Id.*
[20] *Id.*
[21] *Id.*

Comparisons are ranked by the software using a scale of one to ten, and a match is declared based on that rank.[22] Some systems have been programmed to alert a match if the comparison rates at least an "eight," while others have been programmed to alert a match only if the comparison rates a "ten."[23] To ensure accuracy, a human operator monitoring the facial recognition surveillance system compares the face that has been captured by camera to the photograph in the database that has been declared its match.[24] Facial recognition systems marketed by other companies use slightly different methods, but achieve similar results.[25]

B. Use of Facial Recognition Technology in the United States

Widespread implementation of facial recognition technology has yet to be realized in the United States. Even though use is not prevalent here, the capacities in which this software is used in conjunction with video surveillance vary. Facial recognition technology uses include identifying cheaters at casinos and confirming identities of driver's license applicants.[26] The technology has also been used at banks' automated teller machines to protect customers from having fraudulent transactions conducted in their names.[27] Federal, state and local officials may also eventually model their use of facial recognition technology

---

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *See* Graphco Technologies website, *at* http://www.graphcotech.com (last visited October 8, 2001) (on file with the North Carolina Journal of Law & Technology) (providing a description of Graphco's FaceTrac software).
[26] Robert O'Harrow, Jr., *Matching Faces With Mug Shots*, WASHINGTON POST, Aug. 1, 2001, at A01.
[27] *Id.*

after the way other countries use this technology. In Mexico, for example, facial recognition has been used to prevent voter fraud by ensuring that no person votes more than once.[28]

While facial recognition systems have proven successful in these different applications, companies distributing the product emphasize the way that this technology can be used on streets and in other major public areas to identify criminals at large.[29] In order to increase the use of facial recognition systems for this particular purpose, companies have agreed to let selected city law enforcement agencies test their products for free.[30]

Tampa, Florida has benefited from these companies' generous offers of free trial software. It was the first city in the United States to experiment with facial recognition surveillance.[31] The city has utilized facial recognition systems by two different companies.[32]

The system first used by Tampa law enforcement was provided by Graphco Technologies for the Super Bowl.[33] The system was installed in an attempt to comb through the Super Bowl crowd for felons and terrorists.[34] Graphco's software, FaceTrac, operates in much the same way as the FaceIt software manufactured by Visionics Corp.[35] Cameras were installed both

---

[28] Bonsor, *supra* note 14.
[29] O'Harrow, *supra* note 26.
[30] Lane DeGregory, *Click. BEEP! Face Captured*, ST. PETERSBURG TIMES, July 19, 2001, at 1D.
[31] *Id.*
[32] Richard M. Smith, *Digital Frisking in Tampa Must Go* (July 16, 2001), *at* http://www.msnbc.com/news/600153.asp?cp1=1 (on file with the North Carolina Journal of Law & Technology).
[33] *Id.*
[34] Rutherford, *supra* note 2.
[35] Graphco Technologies website, *supra* note 25.

around Raymond James Stadium (the Super Bowl site) and in Tampa's entertainment district, Ybor City.[36] However, such surveillance focused on Super Bowl-related events taking place in and around the stadium. Nineteen individuals with outstanding warrants were identified at the stadium through the facial recognition system, but no arrests were made.[37]

Tampa's city council and law enforcement officials decided to continue using this type of surveillance, but the focus is now on Ybor City rather than on the stadium. In addition to changing its focus, the city has also chosen to switch facial recognition systems. Visionics Corp. has allowed the city to monitor its Ybor City district with its product for one year at no cost.[38] An estimated 125,000 people frequent Ybor City every Friday, and the likelihood that a criminal could be lurking in this crowd is high.[39] Thirty-six video cameras have been installed in this area.[40]

The facial images recorded by the cameras are compared to photographs in three separate databases, which include individuals who are wanted felons, sexual predators, and missing children.[41] The database currently consists of a few hundred photographs which come from existing local law enforcement files, but FaceIt manufacturers plan to expand the database to include 30,000 photographs. [42] A law enforcement officer, operating this system

---

[36] Associated Press, *'Big Brother' Cameras Hit Tampa* (July 2, 2001), *at* http://www.msnbc.com/news/595361.asp (on file with the North Carolina Journal of Law & Technology).
[37] *Id.*
[38] DeGregory, *supra* note 30.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*

at a small, disguised computer center in Ybor City, is responsible for selecting the faces in the crowd that will be turned into faceprints and then compared to the photographs in the databases.[43] As the cameras actively monitor several areas, the officer can manipulate a particular camera's focus by using a computerized joystick mechanism.[44]

After the officer has used the joystick to zoom in on a particular face in the crowd, the software determines if there is an 80 percent or higher probability that a match has been made between the targeted face and a face in the database.[45] If such a match has been made, an alarm sounds prompting the officer to do a visual comparison of the face scanned with the photograph in the database.[46] If the officer's personal scan verifies an accurate match, she now has reasonable suspicion that this person is a wanted criminal or missing child.[47] This allows her to radio officers on the street in Ybor City and have them conduct a temporary stop.[48]

---

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id. See also* Terry v. Ohio, 392 U.S. 1 (1968) (holding that when a police officer observes unusual conduct that leads him to reasonably suspect that criminal activity is at large, he may briefly detain the suspect in order to make inquiries).

IV. Constitutionality of Facial Recognition Video Surveillance Systems

A. Video Surveillance and the Fourth Amendment

Since video surveillance with facial recognition capabilities is a fairly new technological advancement, courts have not yet determined the legality of its use. Federal statutes have not specifically addressed its use either.[49] In addition to the lack of case law and statutes that speak to the use of facial recognition surveillance, the precedent applicable to video surveillance in general is not very helpful.

There are no federal laws that specifically regulate the use of public video surveillance. Lower court decisions on the use of video surveillance rely on Supreme Court rulings on audio surveillance cases.[50] Some courts have also made decisions based on interpretations of federal laws that regulate electronic surveillance but do not address video surveillance specifically.[51] Therefore, in order to determine the legality of facial recognition surveillance, it is important to understand the implications of this technology in the context of the Fourth Amendment. This will allow courts and legislatures to determine if facial recognition surveillance should be allowed the same warrantless use with which general video surveillance has traditionally functioned.

In *Katz v. United States*, the United States Supreme Court held that the Fourth Amendment affords constitutional protection

---

[49] Quentin Burrows, Note, *Scowl Because You're On Candid Camera: Privacy and Video Surveillance*, 31 VAL. U. L. REV. 1079, 1083 (1997).
[50] Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 315 (1999).
[51] *Id.* at 316.

to those areas, both private and public, in which a person reasonably expects privacy.[52] A search impeding an individual's reasonable expectation of privacy requires a warrant or, alternatively, must involve exigent circumstances.[53] The defendant in *Katz* was convicted of illegally conveying gambling information by telephone.[54] The FBI used the defendant's recorded conversations to convict him.[55] The FBI had obtained this evidence by attaching a monitoring device to the outside of the phone booth that Katz regularly used.[56] The Court reasoned that even though the phone booth was in a public area, the Fourth Amendment protects any activity an individual intends to be private, such as the phone conversation the defendant was having inside the phone booth.[57]

The test identified in Katz for determining a lawful search under the Fourth Amendment consists of two parts.[58] First, a subjective expectation of privacy must be held by the individual and second, this privacy interest must be objectively recognized by society.[59]

While the facts in *Katz* involved the unauthorized electronic eavesdropping of oral communications, courts have used the principles pertaining to privacy and the Fourth Amendment established in *Katz* to determine when the use of video surveillance is legally permissible. As discussed previously, an individual's

---

[52] Katz v. United States, 389 U.S. 347, 351 (1967).
[53] *Id.* at 354-56.
[54] *Id.* at 348.
[55] *Id.*
[56] *Id.*
[57] *Id.* at 352-53.
[58] *Id.* at 361 (Harlan, J., concurring).
[59] *Id.*

reasonable expectation of privacy has been the primary factor in determining what activities are deserving of constitutional protection. Courts have upheld the use of video surveillance without a warrant in places where individuals do not have a reasonable expectation of privacy such as public streets and sidewalks, employee work areas, and public school classrooms.[60]

This lack of a reasonable expectation of privacy in the realm of public video surveillance can be based upon the plain view doctrine established by the Supreme Court one year after *Katz* in *Harris v. United States.*[61] The Court stated, "it has long been settled that objects falling in the plain view of an officer who has the right to be in the position to have that view are subject to seizure and may be introduced in evidence."[62]

The plain view doctrine, as discussed in *Harris,* has often been used to determine that video surveillance of most public areas does not constitute an unreasonable search under the Fourth Amendment.[63] Public video surveillance equates to activity falling

---

[60] Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 184 (1st Cir. 1997) (holding that "employees do not have an objectively reasonable expectation of privacy in the open areas of the workplace"); United States v. Vazquez, 31 F. Supp. 2d 85, 91 (Dist. Conn. 1998) (holding that a common law right to privacy does not extend to public streets and sidewalks because no one in these areas has a legitimate expectation of privacy); State v. McLellan, 744 A.2d 611, 615 (N.H. 1999) (holding that a classroom is not a private place in which an individual could reasonably expect to be safe from surveillance).

[61] United States v. Harris, 390 U.S. 234 (1968).

[62] *Id.* at 236.

[63] *Vega-Rodriguez,* 110 F.3d at 180; Int'l Union v. Garner, 601 F. Supp. 187, 191 (M.D. Tenn. 1995) (holding that an "individual has no right to expect that persons passing by on the street will not take note of -- and draw inferences from -- the presence of the individual's car parked on the street in plain view for all to see").

within the plain view of an officer since such surveillance cameras have been deemed the equivalent of robotic police officers.[64] The video surveillance does not capture any activity that a human police officer could not have seen with her eyes had she been in the public area where the activity was taking place.

In addition to using the principles established in *Katz,* courts have looked to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Crime Act") to determine the legality of video surveillance.[65] Title III was enacted in response to *Katz* and is the closest that Congress has come to specifically regulating video surveillance.[66] Interception of electronic, wire, and oral communications is specifically regulated by Title III, but video surveillance without audio capabilities is not.[67] Therefore, silent video surveillance, which would encompass the majority of cameras being used to monitor public areas, is left unregulated. Some court decisions have interpreted this legislative silence to mean that Title III is not applicable to video surveillance.[68] Other courts have made video surveillance search warrant requirements comparable to the requirements set out by Title III.[69]

---

[64] SCOTT SHER, CONTINUOUS VIDEO SURVEILLANCE AND ITS LEGAL CONSEQUENCES, Public Law Research Institute Report, University of California-Hastings College of Law Working Papers Series (Fall 1996).

[65] United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); United States v. Torres, 751 F.2d 875 (7th Cir. 1984).

[66] Burrows, *supra* note 49, at 1096.

[67] 18 U.S.C. 2518 (2001).

[68] United States v. Falls, 34 F.3d 674 (8th Cir. 1994); Thompson v. Johnson Cmty. Coll. Dist., No. 96-3223, 1997 U.S. App. LEXIS 5832 (D. Kan. March 25, 1997).

[69] *Biasucci,* 786 F.2d at 510 (holding that "these standards, borrowed from Title III, together with the more general constitutional requirements, form a sufficient

B. Facial Recognition Video Surveillance Systems and the Fourth Amendment

Courts have found repeatedly that warrantless video surveillance of public areas does not violate the Fourth Amendment, and it seems likely that courts will take the same approach toward public surveillance systems incorporating facial recognition software. At first glance, the use of facial recognition technology in this manner may constitute an unreasonable invasion of an individual's privacy due to its great degree of intrusion. In a sense, all individuals in the camera's path are subject to a police lineup.[70] This lineup is also extremely advanced because, as discussed previously, it provides police with information such as the width of an individual's nose and the depth of an individual's eye sockets. This is not detectable by mere eyesight but requires measuring devices.[71] So while individuals may have no reasonable expectation of privacy when they utilize public spaces, such as shopping malls, parking lots, and airports, it would seem that they would have a reasonable expectation of privacy in these same areas when facial recognition systems are used to monitor their behavior. However, the constitutionality of facial recognition technology may not be so clear-cut.

---

outline of the showing the government must make before a warrant should issue authorizing video surveillance").

[70] Martin Kasindorf, *'Big Brother' Cameras on Watch for Criminals* (Oct. 2, 2001), *at* http://www.usatoday.com/life/cyber/tech/2001-08-02-big-brother-cameras.htm#more (on file with the North Carolina Journal of Law & Technology).

[71] Bonsor, *supra* note 14.

As intrusive as facial recognition technology appears to be, it must be determined if its use in a public area is so intrusive as to constitute an unreasonable search and entitle individuals to Fourth Amendment protection as just suggested. The two-part test established in *Katz* to determine an individual's reasonable expectation of privacy in a particular situation balances an individual's privacy interests with society's need for law enforcement to maintain order.[72] When considering the balancing test for reasonableness of searches, the intrusiveness of facial recognition systems in public areas may not infringe on an individual's reasonable expectation of privacy as much as it ensures society's safety.

1. Physical Intrusion

A determinative factor in this balancing test is assessing if the use of facial recognition constitutes a physical intrusion upon an individual's body. Drawing blood, taking urine samples, and imposing a breathalyzer test all have been found to be Fourth Amendment searches, therefore requiring a warrant or exigent circumstances.[73] If facial recognition technology is comparable to these bodily invasions, using it would constitute a search. If this is the case, warrantless use of this technology could only occur if both exigent circumstances existed and it was obvious that fundamental evidence would be obtained.[74]

It is unlikely that a court would consider the use of facial recognition systems to monitor public areas a search based on its

---

[72] SHER, *supra* note 64.

[73] Woodard, *supra* note 9, at 124.

[74] ROLANDO V. DEL CARMEN, CRIMINAL PROCEDURE: LAW AND PRACTICE 181 (2d ed. 1991).

level of physical intrusiveness. When an individual's face is subjected to an in-depth computerized analysis, no actual physical intrusion on the body is being made. In fact, an individual does not need to knowingly surrender anything of the person for the system to work. Therefore, this level of intrusiveness does not actually invade a person's reasonable expectation of privacy in light of government interests.

2. Plain View

An analysis of facial recognition surveillance under the *Harris* plain view doctrine also suggests that it would pass muster under the *Katz* two-part test. *Harris* should apply to these systems in much the same way it applies to general public video surveillance systems. These facial recognition systems monitor public areas in which a person does not have a reasonable expectation of privacy because he is knowingly placing himself in plain view of other people, as well as the cameras. Arguably, with the facial recognition system, the camera is doing more than just monitoring what is in plain view of its lens. However, the Supreme Court has held various technological devices that have been used to enhance law enforcement's senses to be constitutional.[75]

[75] Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that the warrantless taking of photographs from an aircraft lawfully in the public airspace that is sufficiently near the reach of the cameras does not constitute a search); United States v. Knotts, 460 U.S. 276, 285 (1983) (holding that a driver's reasonable expectation of privacy is not violated with law enforcement's use of an electronic device to follow his vehicle on the public roads); Texas v. Brown, 460 U.S. 730, 740 (1983) (holding that "the use of

3. Sensory Enhancing Devices

The Supreme Court has held that Fourth Amendment protection does not extend to law enforcement's warrantless observations made from public property through such sensory enhancing devices as flashlights, electronic tracking devices, and aerial cameras.[76] The rationale provided by the Supreme Court is that observations with these devices are made from areas where police have the right to be, and the observations could be made with "plain view" surveillance performed without the device.[77] In June 2001, the Supreme Court differentiated the use of sensory enhancing technology in some situations in *Kyllo v. United States*.[78] In *Kyllo*, the police suspected that the defendant was growing marijuana inside his home with the use of high-intensity lamps.[79] The police used a thermal imaging device to determine if the exterior of defendant's home was emitting a significant amount of heat that would be consistent with the amount of heat generated by the high-intensity lamps.[80] The Court stated, "Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[81]

---

artificial means to illuminate a darkened area simply does not constitute a search, and thus triggers no Fourth Amendment protection").

[76] *Id.*

[77] *Knotts*, 460 U.S. at 281.

[78] Kyllo v. United States, 533 U.S. 27, 121 S. Ct. 2038 (2001).

[79] *Kyllo*, 121 S. Ct. at 2041.

[80] *Id.*

[81] *Id.* at 2046.

In reaching its decisions, the Court focused on two issues: that the inside of an individual's home is so intimate as to give her a reasonable expectation of privacy and that the general public is not aware that their privacy can easily be invaded through such technology.[82]

The warrantless use of facial recognition software with public video surveillance appears lawful in that it is consistent with these Supreme Court decisions on sensory enhancing devices. The cameras monitor public areas to which enforcement officers have access, and the observations made with the facial recognition system could be made without its use. Using this system is the equivalent of officers observing a crowd and comparing the faces in it to those in a criminal face book; it is just much faster and may be more accurate.[83] Based on this analogy, facial recognition surveillance, like general video surveillance, can be viewed as the equivalent of a robotic police officer.

Even though *Kyllo* has narrowed the circumstances in which warrantless use of advanced technology can be used to conduct a search, public video surveillance systems using facial recognition software remain within the realm of these circumstances. Although facial recognition technology is not in general public use, utilizing this technology with public surveillance is not so invasive because it does not intrude upon an area in which an individual has a reasonable expectation of privacy. The Supreme Court suggests that both criteria need to be met in order to trigger Fourth Amendment protection. Accordingly, if this technology were to be used to determine the

[82] *Id.* at 2043-44.
[83] Milligan, *supra* note 50, at 319.

identities of individuals within a home or another private area, then it is likely that such use would require a warrant as well.

C. Constitutionality In Light of Threats to National Security

There appears to be only one context in which the use of facial recognition technology in this manner poses no constitutional questions. This context is the use of facial recognition systems in response to a threat to national security. In a footnote, the *Katz* majority alluded to the idea that this type of circumstance may have changed the outcome of the case by stating that "a situation involving the national security is a question not presented by this case."[84] This suggests that there may be situations in which a search that ordinarily would be considered unreasonable under the Fourth Amendment could be conducted without a warrant and still be regarded as having been constitutionally valid. The Omnibus Crime Act also provides for exceptions to the warrant requirement in light of emergency situations, such as threats to national security.[85]

The USA PATRIOT Act of 2001, signed into law on October 26th, has also expanded the government's surveillance capabilities in order to protect the country in its current state of crisis following the September 11th terrorist attacks.[86] The Act provides federal agents with new and expanded powers, mainly by eliminating the system of checks and balances that had been previously used by courts to regulate these powers.[87] Previous

[84] Katz v. United States, 389 U.S. 347, 359 (1967).
[85] 18 U.S.C 2518(7)(a) (2001).
[86] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
[87] *Id.*

restrictions on how agents could tap a suspect's phone or conduct secret searches of a suspect's home have now been softened.[88]

While the Act does not specifically regulate video surveillance or facial recognition technology, it is possible that courts will apply its provision to such technology in much the same manner as the Omnibus Crime Act's Title III has been deemed applicable to silent video surveillance. For example, because the Act has relaxed some of the previous warrant requirements to conduct secret searches, it is possible that facial recognition surveillance could be used secretly at a suspect's home to identify other suspects.

V. Conclusion: Safeguards for Facial Recognition Surveillance

This country could see widespread use of public facial recognition surveillance in response to the September 11th tragedy. Even though constitutional issues surrounding the use of this type of surveillance under ordinary circumstances are unresolved, implementation of this surveillance in certain situations may be necessary to protect our country from future terrorist attacks of a similar nature.

In the weeks following the tragedy, facial recognition was the topic of discussion in various news forums. Proponents for and against the use of facial recognition have voiced their opinions. Supporter Richard Chace of the Security Industry Association said upon seeing videotape footage of one of the terrorists walking through a terminal at Logan International Airport, he knew that had the security cameras that had taken the footage been equipped with facial recognition technology, this particular hijacking might

[88] *Id.* at §§ 206, 213.

have been prevented.[89] However, opponent Howard Simon, Executive Director of the Florida ACLU, has stated his belief that this type of surveillance will perpetuate the practice of racial profiling.[90] Recognizing these concerns, safeguards need to be in place even though the country's current circumstances clearly warrant use of this technology. Safeguards are also necessary if it is later determined that this type of technology is constitutional under normal circumstances.

One of these necessary safeguards would involve placing restrictions on where this type of surveillance could be used. This would limit some of the intrusiveness that would be experienced with widespread implementation of this technology. This restriction would also prevent the police from targeting specific communities that are stereotypically identified as high crime areas, such as low income and minority communities.[91] The use of facial recognition surveillance should be limited to major public areas, primarily major transportation centers like airports, bus and train terminals, subways, and car rental agencies.[92] This surveillance should also be implemented at government buildings and at our country's major economic centers like the Department of Justice and the Sears Tower. Considering the manner in which the

---

[89] *The Today Show* (NBC television broadcast, Sept. 27, 2001).

[90] Press Release, ACLU Freedom Network, ACLU Probes Police Use of Facial-Recognition Surveillance Cameras in Florida City, ACLU Freedom Network, July 6, 2001, available at <www.aclu.org/news/2001/n070601a.html>.

[91] Milligan, *supra* note 50 at 328 (discussing how public video surveillance was first used for law enforcement purposes on Miami Beach only after the once elderly community experienced lower income Black and Latino citizens moving into it).

[92] *See* Addie S. Ries, Comment, *America's Anti-hijacking Campaign—Will It Conform to Our Constitution?*, 3 N.C. J.L. & TECH. 123 (2001), elsewhere in this issue.

September 11th terrorist attacks were carried out, these are ideal locations for such surveillance systems.

It appears the government is already looking into such use. The Department of Transportation committee responsible for restructuring airport security met with the president of Visionics Corp., Joseph Atick. Atick and the committee discussed how airport security cameras could utilize FaceIt software.[93] The facial images recorded by camera would be compared with a database of photos of known or suspected terrorists.[94] Government officials at a federal monitoring station would be notified of a potential match instantly through the Internet.[95] After their involvement with the September 11th tragedy, Washington D.C.'s Reagan National Airport and Boston's Logan International Airport have been identified by government officials as potential sites for initial implementation of facial recognition systems.[96] Facial recognition systems were also purchased by or donated to at least two other U.S. airports in the three months following September 11th, so the Department of Transportation decided that the surveillance is legal.[97]

In addition to limiting the locations where facial recognition surveillance systems would be used, the systems' uses

---

[93] Robert O'Harrow, Jr., *Facial Recognition System Considered For U.S. Airports*, WASHINGTON POST, September 24, 2001, at A14.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *See* Associated Press, *Hi-tech Interrogation Comes to OAK* (Oct. 19, 2001), *at* http://www.msnbc.com/local/kntv/m105587.asp (on file with the North Carolina Journal of Law & Technology); Associated Press, *State of the Art Security System Tested at Fresno Airport, at* http://www.msnbc.com/local/ksee/a13001.asp (on file with the North Carolina Journal of Law & Technology).

could be further limited if the photo databases only contain the images of known or suspected terrorists. By limiting the category of criminals that are being monitored with this system, the opportunity for a police officer to operate this system in a biased manner is lessened. A facial recognition surveillance system, operating in much the same way as that in Tampa's Ybor City, would be monitored and operated by a police officer. Because the police officer selects those faces that are going to be scanned into the system, there is the potential that the officer would scan only those faces he associates with a criminal profile. More often than not, the faces that are associated with that profile are the faces of minorities.[98] Even limiting the database to photographs of known or suspected terrorists may lead to the racial profiling of individuals of Arab descent.[99] A much-needed safeguard would involve decreasing the amount of human element involved in this surveillance system. Rather than having the police officer who is monitoring the surveillance system choose which faces will be scanned into the system, the system itself could be designed to control that decision.

It is obvious the most needed safeguard for facial recognition technology is the implementation of federal regulations to monitor its use or a Supreme Court decision on its constitutionality. With facial recognition going into United States airports, the likelihood is great that the constitutionality of its use will be challenged soon in the judicial system. Federal law or

---

[98] *See* John Stossel, *Rethinking Racial Profiling: How the Attacks Have Changed Views* (Oct. 3, 2001), *at* http://abcnews.com/sections/2020/2020/2020_011002_racialprofiling_stossel.html (on file with the North Carolina Journal of Law & Technology).

[99] *Id.*

regulations may soon be implemented as well.[100] However, until such are in place, law enforcement, airport security, and other agencies that utilize facial recognition technology should proactively ensure that society will benefit from its use. This technology has the potential to provide citizens with increased safety, but it also has the potential to unreasonably invade their privacy.

[100] *See* Ries, *supra* note 92.