Winter 2002


Robert H. Thornburg

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation


http://repository.jmls.edu/jitpl/vol20/iss2/5

This Comments is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
FACE RECOGNITION TECHNOLOGY:
THE POTENTIAL ORWELLIAN
IMPLICATIONS AND
CONSTITUTIONALITY OF
CURRENT USES UNDER
THE FOURTH AMENDMENT

I. INTRODUCTION

In the classic novel 1984, George Orwell described a totalitarian society where each room had a built-in camera and where Big Brother, the government, conducted surveillance on its citizens. In the last few years, face recognition technology, a computer enhanced video surveillance system, has been developed as the security method to help identify known terrorists and criminals. While this technology has the potential to help increase security in public venues to deter criminals and to make our lives more safe, commentators have been quick to point out that this advance could be nothing more than the next step in implementing a society not much different than that envisioned by George Orwell.

Face recognition technology has already been used upon unknowing spectators at the 2001 Super Bowl at Tampa's Raymond James Stadium. The technology has been implemented in two locations, Tampa's Ybor City entertainment district and the hockey arena of the Salt Lake City Winter Olympics, only to be discontinued due to ineffectiveness. Although there has never been a successful implementation of a facial recognition system, and while there has never been a terrorist or wanted criminal arrested due to these systems, the technology continues to be a hot topic of discussion by privacy advocates.

3. Id. at ¶ 4.
While face recognition technology would have continued to be a hotly debated topic in this country, emphasis on such potentially privacy evading systems changed with the tragic events of September 11th.\textsuperscript{6} The terrorist plots in both New York and Washington did more than just awake a nation as to the growing problems of terrorist states, it quickly alerted a need for increased security in our airports, which has directly resulted in disrupting the traditional balance between individual privacy and public safety. With this increased need for security in domestic air travel, airports have quickly turned to implementing face recognition technology.\textsuperscript{7}

It remains unclear whether face recognition technology constitutes a system which society would regard as a reasonable intrusion into their privacy. As a technology still in its infant stages, privacy advocates are simply left to wonder about the potential uses and future constitutional implications of face recognition technology. No federal regulation or case law directly on point exists to provide any guidance on how to implement this technology in a manner that protects an individual's constitutional rights. Thus, without such constructs to allow protection of the public, privacy advocates will have to continue to assess the intrusiveness of this governmental technique to protect against the potential of a Big Brother government, similar to that described by George Orwell in \textit{1984}.\textsuperscript{8}

This paper seeks to explore both the actual uses of this technology and the constitutionality of face recognition systems under the Fourth Amendment. In Part II of the paper, the evolution of face recognition is discussed from the initial development of video surveillance to the recent use of face recognition systems at the Salt Lake City Winter Olympics. Part III concentrates on how to assess whether a technology-enhanced government method constitutes a search under the Fourth Amendment, and thus whether such a method offends an individual's legitimate expectation of privacy. Part IV applies these constructs to the potential uses of face recognition technology, and provides potential reasoning of whether the method offends the traditional notions of privacy under the Fourth Amendment. Finally, Part V concludes the paper with a discussion of the potential impact of the tragic events of September 11\textsuperscript{th} could have on society's objective view of face recognition technology, whether it


\textsuperscript{8} Nick Schoon, \textit{Caught on Camera: Digital Face Recognition} \url{<http://www.countdown.org/end/big_brother_07.htm>} (last updated Dec. 1999).
could accept such methods as reasonable, and the role of advocates and commentators in this process.

II. THE HISTORIC DEVELOPMENT OF FACE RECOGNITION TECHNOLOGY

A. INTRODUCTION TO BIOMETRIC TECHNOLOGY

The progeny of face recognition technology began in the banking industry with the initial development of video surveillance. First introduced in 1956, video surveillance technology has grown into widespread use in many public venues such as shopping malls, at ATM machines, and in convenience stores. With the dawn of the age of digital imaging, these devices became more effective, less expensive, and more prevalent throughout the country. In 1982, the City of Miami Beach implemented one of the country's first large scale deployment of video surveillance to protect its prime retail shopping district due to lack of adequate police personnel. Today, Americans are constantly subjected to video surveillance in various forms including crime prevention, productivity monitoring, and safety programs. Over sixty urban centers in the United States use video surveillance in public places, with Baltimore boasting "the most expansive system currently in place."

As with these advancements in video surveillance, the last twenty years has seen tremendous advances in biometric technologies. "Biometrics" encompass "the techniques and methods used to identify [an] individuals based on [his or her] physical characteristics." The technology "generally consists of four steps": (1) a "physical characteristic [or trait] is scanned", (2) those "unique features are converted into a digital code", (3) "the code is then stored in a database" or another retrievable form, and (4) that database and digital code are accessed to identify the individual at a later time. Technologies currently utilizing biometric

11. Bennett, supra n. 9, at 153.
13. Id.
17. Id. at 445.
identifiers include facial imaging, hand geometry, voice recognition, and retinal scans.\textsuperscript{18} 

The benefit of these technologies stem from their ability to accurately identify a person entering a facility through scanning their unique physical characteristics.\textsuperscript{19} This ability is paramount in government and private research facilities that house highly secure items such as weapons, nuclear and biohazardous materials, and top-secret information.\textsuperscript{20} Also, advocates of biometric technologies hail these advances as having numerous advantages for consumers, like reducing instances of consumer fraud,\textsuperscript{21} speeding lines at airports check-in,\textsuperscript{22} and deterring criminals from entering public areas employing the technologies.\textsuperscript{23} However, while commentators have found some benefits from these identification methods, privacy advocates such as the Electronics Privacy Information Center and the American Civil Liberties Union ("ACLU") have warned of the potential constitutional implications of these emerging technologies.\textsuperscript{24} 

While face recognition technology has always been at the forefront of these emerging biometric identification tools, both government and private research in the field has greatly accelerated over the past ten years.\textsuperscript{25} Over this span, both university scientists and the Department of Defense have worked hand-and-hand to make face recognition technology a reality.\textsuperscript{26} As the research and development agency of Department of Justice, the National Institute of Justice since 1997 "has spent [over] eight million dollars [in] developing face recognition technologies through [their independent] think tank, ANSER."\textsuperscript{27} The government's

\begin{itemize}
  \item \textsuperscript{18} Id. at 447.
  \item \textsuperscript{19} Woodard, supra n. 15, at 97, 100.
  \item \textsuperscript{20} Philip E. Agre, Your Face is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places ¶ 2 <http://dlis.gseis.ucla.edu/people/pagre/bar-code.html> (last updated Jan. 28, 2002).
  \item \textsuperscript{21} Rachel Konrad, Airport Security Technology Under Scrutiny ¶ 6 <http://news.com/21001001-272938.html> (Sept. 12, 2001). Currently, Walt Disney World in Orlando has begun implementing hand recognition devices in entrances at the Orlando theme park in order to reduce instances of individuals sharing season passes. \textit{Id.}
  \item \textsuperscript{22} \textit{Id.}
  \item \textsuperscript{23} USA Today, Tampa Puts Face-Recognition System on Public Street ¶ 11 <http://www.usatoday.com/life/cyber/tech/2001-07-13-tampa-surveillance.htm> (last updated July 13, 2001) [hereinafter \textit{Tampa Puts Face-Recognition}]. In implementing face recognition technology in the Ybor City entertainment district of Tampa, city council members supported the initiative asserting that the technology would deter known criminals from entering the district for fear of being identified. \textit{Id.}
  \item \textsuperscript{24} Konrad, supra n. 21, at ¶ 14.
  \item \textsuperscript{25} Agre, supra n. 20, at ¶ 1.
  \item \textsuperscript{26} Bennett, supra n. 9, at 154.
  \item \textsuperscript{27} Julia Scheeres, Your Face-Scan Dollars at Work ¶ 3 <http://www.wired.com/news/technology/0,1282,46018.html> (Aug. 15, 2001). "Headed [up] by the former CIA deputy
initial interest has been to potentially implement this technology to patrol the country's borders to reduce illegal immigration, to identify suspects during mobile stakeouts, to scan the Internet for missing children, to help search for pedophiles and purveyors of child pornography, and the general identification of wanted criminals.

B. HOW FACE RECOGNITION TECHNOLOGY WORKS

Facial recognition technology is comprised of two important components, the video surveillance cameras used to obtain a snapshot of an individual's face, and the computer software used to extract and analyze that face for identification purposes. Developed by Visionics of Jersey City, N.J, the FaceIT technology used in the Ybor City District of Tampa, employs mounted cameras used to scan crowds to extract a single human face. The Visionics "software uses a variety of pattern matching algorithms to determine if a face is" in view of the cameras. Once detected, the human face is extracted from its surroundings and the digitized face is filtered to remove variations, including changes in lighting and facial expression.

The program then uses this digital template to measure over eighty nodal points that comprise an individual's face such as the distance between eyes, width of the nose, and depth of the eye sockets.

The result of this analysis is a set of numerical data called a faceprint. Note that not every nodal point can be accurately measured based on the template acquired by the captured digital image. Thus, the software is programmed to use between fourteen and twenty-two of

director of science and technology, Ruth David," ANSER is a fifty-year old government think tank that develops law enforcement technology. Id.

28. Bennett, supra n. 9, at 154.
29. Scheeres, supra n. 27, at ¶ 7.
30. Id. at ¶ 6. Developed as one of the programs created by the National Institute of Justice, the Missing Child Locator employs facial recognition technology to continually scan the Internet for images that may potentially match with missing children. Id.
31. Id. at ¶ 11.
32. Id. at ¶ 7.
34. Tampa Puts Face-Recognition, supra n. 23, at ¶ 1.
36. Id. at ¶ 2.
38. Bennett, supra n. 9, at 155.
39. Id. at 156.
the measured nodal points in creating the numerical faceprint.\textsuperscript{40} If there are sufficient nodal measurements to create a faceprint, the computer then accesses a stored database of faceprints. Often, individual FaceIT programs allow a human operator to assess the captured photograph with the potential match found by the software.\textsuperscript{41}

C. Implementation of Face Recognition Technology Within the United States

1. The Super Bowl and Ybor City

While the use of face recognition technology has been limited in the United States, its implementation has been tied with major sporting events and other highly publicized uses. In January 2001, cameras were placed throughout Raymond James Stadium by the Tampa Police Department, to scan the faces of unsuspecting Super Bowl fans.\textsuperscript{42} Graphco Technologies donated the system as an initial demonstration of the effectiveness of the face recognition technology.\textsuperscript{43} Facial images acquired by the technology were transferred to computers at a Tampa police command post in Raymond James Stadium and compared with a large database of suspected criminals and known terrorists.\textsuperscript{44} The technology did successfully identify nineteen petty criminals out of almost 100,000 fans, but no arrests were actually made by Tampa police.\textsuperscript{45} While the Super Bowl was the first successful demonstration of face recognition technology at a major sporting event, the use drew heavy criticism from the ACLU, since none of the spectators attending the event were aware before or during the game, that the technology had been used.\textsuperscript{46}

In addition to the Super Bowl, the Tampa city counsel and law enforcement officials opted to employ face recognition technology in its Ybor City entertainment district.\textsuperscript{47} Historically known as a high crime area, an estimated 125,000 people visit the district every Friday.\textsuperscript{48} On June 29, 2001, Tampa police installed several dozen cameras along Seventh Avenue of Ybor City, using the FaceIT technology developed by Vi-

\begin{itemize}
  \item \textsuperscript{40} Id. at 155.
  \item \textsuperscript{41} Id.
  \item \textsuperscript{42} Jack Carey, ACLU Protests High-Tech Super Bowl Surveillance ¶ 2 <http://www. usatoday.com/life/cyber/tech/2001-02-02-super-bowl-surveillance.htm> (last updated Feb. 6, 2002).
  \item \textsuperscript{43} Bennett, supra n. 9, at 157.
  \item \textsuperscript{44} Id.
  \item \textsuperscript{45} Id. at 158.
  \item \textsuperscript{46} Carey, supra n. 42, at ¶ 2.
  \item \textsuperscript{48} Tampa Puts Face-Recognition, supra n. 23, at ¶ 1.
\end{itemize}
However, while the Visionics system provided fourteen possible matches in the first few days of operation, none were actually correct identifications. In fact, two of these matches were actually of persons of the opposite sex. Because the system had failed to correctly identify a single face in the Tampa police's database of criminal suspects, the Ybor City system was officially suspended on August 11, 2001.

2. The Use in Airports After September 11th

Apart from Tampa, the nation’s airports have increased their interest in using facial recognition technology after the events of September 11, 2001. Soon after the devastating airline crashes in New York and Washington, D.C., the Department of Transportation contacted Visionics about the potential of using the FaceIT technology in our nation’s airports. In addition to Visionics, airport executives began looking at the technology developed by Viisage, Inc., a technology start-up company based out of Massachusetts Institute of Technology (“MIT”). The Federal Aviation Association (“FAA”) soon began to test and evaluate the different companies developing face recognition technology to assess which would be the most effective to meet airport security needs. Implementing the software and systems in a major U.S. airport, such as Logan International, could total almost $500,000.

In January 2002, both Fresno International Airport and St. Petersburg-Clearwater International Airport implemented Viisage’s FaceFINDER technology. Operated by the Pinellas County Sheriff’s Office, St.-Petersburg-Clearwater International Airport checks ticketed passengers against a database containing Federal, State, and local area criminals. Around the same time, Visionics announced that Dallas/Fort Worth, Boston Logan, and Palm Beach International Airports

49. Stanley, supra n. 37, at ¶ 2.
50. Id. at ¶ 14.
51. Id.
52. Id. at ¶¶ 13, 26.
53. Konrad, supra n. 21, at ¶¶ 2, 8.
57. Fenoglio, supra n. 55.
59. Id. at ¶ 3.
would begin testing of its FaceIT technology at security checkpoints. Technology forecasters predict that by 2005, technology companies developing face recognition technology for use in airports will have revenues approaching $1.9 billion.

3. Use by Casinos

Besides the potential as a security measure in domestic airports, face recognition technology has found use at various casinos, helping casino owners identify known cheats. “When the New York- New York Hotel & Casino opened in Las Vegas in 1997,” its casino surveillance system already included face recognition technology, which has operated 24-hours a day ever since its opening. Soon after, the Viisage Technology was implemented in the Foxwood Casino in Connecticut, and several other Las Vegas casinos began using the Visionics FaceIT system. On March 29, 2000, Viisage announced the fiftieth order and installation of its surveillance system at a casino when it installed the system at the Mirage Resort in Las Vegas. Within three years, the number of Las Vegas casinos using facial recognition systems grew from a handful to over ninety casinos, “ranging from the small Native American owned facilities to” the more well-known hotel and casinos. The Casino Information Network (“CIN”) allows casino security operators at independent casinos to tap into a large private biometric database of shared pictures in order to identify cheats recently evicted from area casinos.

4. The Salt Lake City Winter Olympics

Apart from the over 15,000 troops amassed by U.S. forces as security measures for the Salt Lake City Winter Olympics, face recognition tech-
nology was used to scan crowds for possible terrorists.68 "Of the reported $1.9 billion budget for the Salt Lake Games," organizers spent $310 million on security measures, including facial recognition technology.69 At the opening ceremonies of the games, Federal Bureau of Investigation ("FBI") agents scanned the 52,000 spectators, cross checking them with criminal mugshots.70 Because of both public criticism and spiraling security costs, face recognition technology was not implemented in every Olympic venue.71 The AcSys system, developed by the AcSys Biometrics Corporation in Burlington, Canada, was installed in two locations to prevent unauthorized access to where the Olympic medals were kept, and at both the men's and women's hockey games.72 However, because of concerns that the technology was not working properly, the system was shut down at the Olympic Hockey venue.73

D. INTERNATIONAL USE OF FACE RECOGNITION TECHNOLOGY

The use of face recognition technology has not been limited domestically, and several countries have begun looking toward the technology to aid in banking surveillance, prevent voter fraud, and in increased security efforts in airports. Biometric technology has traditionally been more accepted overseas, with greater use in International Airports.74 By August 2001, Visionics reported doing business with almost sixty nations.75 While the company has agreed to implement its technology in China to aid in security of the nation's banking industry, the company has denied

68. Tightest Security Ever for Games, The Advertiser (South Australia) § Sports (Feb. 8, 2002).
69. David King, Security Becomes an Olympic Undertaking; Making Salt Lake City Safe for Games is Taking $310 million, 15,000 People and an Array of High-Tech Gear, San Antonio Express, News A1 (Feb. 6, 2002).
70. Michael Beach, Troops Outnumber Athletes, Courier Mail, § News (Feb. 9, 2002).
72. Mark McNeil, Nexus Earns Games Berth; Face Recognition System Will Scan Hockey Crowds, Protect Medals Vault, Hamilton Spectator (Ontario, Canada) C01 (Feb. 7, 2002). While many privacy advocates argued against the use of face recognition technology at the Winter Games, Nexus Group International, the company which owns AcSys Biometrics Corporation, argued that since its software does not retain the facial images it acquires while scanning, that the method does not violate individual privacy. Id.
73. Hi, Mom, Say Hello to President Bush, St. Petersburg Times C19 (Feb. 10, 2002).
74. Erica Vonderheid, Biometrics Verify Travelers' Identity, 26 Institute 6 <http://www.spectrum.ieee.org/INST/jan02/fbio.html> (last updated Jan. 2002). Tel Aviv's Ben Gurion Airport has used a biometric technology since 1998 that scans palm prints which compares the print to information stored on a passenger's "smart card." Id. In addition, Amsterdam's Schiphol airport uses eye-scanning technology at its security checkpoints, also comparing with an image taken from a passenger's photographic identification. Id.
sales to certain nations such as Iraq, Iran, and Libya.\textsuperscript{76} In an implementation similar to Ybor City, Visionics contends that the use of face recognition technology in the Newham Borough of London has led to a forty percent reduction in crime.\textsuperscript{77} Keflavik International Airport in Iceland was the first airport to actually use the technology.\textsuperscript{78}

One unique foreign use of face recognition technology has been to prevent voter fraud. In the July 2000 Mexican presidential elections, MetaData, a Mexico City-based Visionics’ partner, expanded the FaceIT software to help eliminate duplicate voter registrations.\textsuperscript{79} In a similar use, Viisage implemented its technology during the recent national election in the Republic of Uganda.\textsuperscript{80} The system used a database containing almost ten million images.\textsuperscript{81}

\textbf{III. CONSTITUTIONALITY OF TECHNOLOGY ENHANCES GOVERNMENT METHODS}

While there is no state or federal case law that addresses the constitutionality of face recognition technology, a court would have to focus on whether it constitutes a search under the Fourth Amendment. The Fourth Amendment provides that “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 on probable cause.”\textsuperscript{82} In\textit{ Katz v. United States}, Justice Harlan, in his concurring opinion, outlined the two essential inquiries in whether a person has a constitutionally protected expectation of privacy under the

\textsuperscript{76} Id. at ¶ 4, 6


\textsuperscript{80} Matthew French, \textit{Recognition Technology Adds Security} ¶ 2 <http://www.masshightech.com/as-mazzu.asp> (Mar. 8, 2002).

\textsuperscript{81} Id.; Julia Scheeres, \textit{Plot Intimidates Uganda Voters} ¶ 2 <http://www.wired.com/news/print/0,1294,42070,00.html> (Feb. 27, 2001). However, law professor Winston Nagan at the University of Florida, cautioned that the methods used by Viisage, namely the taking of digital photographs before voters entered polling booths, could have lead to intimidation of Ugandans, and thus reduce voter turnout. \textit{Id.}; David McGuire, \textit{Urgandan Voter Biometrics Could Violate Privacy} ¶ 6 <http://www.infowar.com/classl/01/class1_030501a_j.shtml> (Mar. 2, 2001). Furthermore, privacy advocates at the Center for Democracy and Technology assert that the secret ballot is a key element to democratic elections, and that the use of face recognition technology puts this element of the voting process in jeopardy. \textit{Id.}

\textsuperscript{82} U.S. Const. Amend. IV.
Fourth Amendment.\textsuperscript{83} First, courts look to whether an individual has manifested a "subjective expectation of privacy" in the object of the challenged search.\textsuperscript{84} Second, courts evaluate whether society is willing to recognize that expectation as "reasonable."\textsuperscript{85}

In assessing whether an individual has a legitimate expectation of privacy, the Supreme Court has consistently asserted that purely visual inspections are less intrusive, and thus less likely to constitute a search, compared to more tactile or physical invasions.\textsuperscript{86} For example, the Supreme Court in \textit{Terry v. Ohio} has asserted that a careful frisk of the outer surfaces of a person's clothing constitutes a "serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment and is not to be undertaken lightly."\textsuperscript{87} On the other hand, just one year after \textit{Katz} the Supreme Court asserted in \textit{Harris v. United States} that "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."\textsuperscript{88}

A. Subjective Expectation of Privacy with Video Surveillance

When looking at whether an individual has demonstrated a subjective expectation of privacy not to be recorded in video surveillance, courts look to whether that individual's conduct shows that he or she seeks to preserve such activities as private.\textsuperscript{89} Under this inquiry, the court must assess the person's state of mind in assessing whether their actions showed such subjective expectation.\textsuperscript{90} While the Supreme Court has not developed a specific checklist to assess whether a person shows a subjective expectation, it has addressed the question employing diverse factors such as the use to which an individual has put a location, and society's understanding that certain areas deserve a heightened protection from government intrusions.\textsuperscript{91} When recently assessing whether an individual had a subjective expectation regarding luggage aboard a bus, the Supreme Court focused on the individual's use of an opaque bag to conceal materials he was traveling with, in asserting the individual had demon-

\begin{itemize}
\item \textsuperscript{83} 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
\item \textsuperscript{84} Id.; see Cal. v. Ciraolo, 476 U.S. 207, 211 (1986).
\item \textsuperscript{85} \textit{Katz}, 389 U.S. at 360 (Harlan, J., concurring); \textit{Smith v. Md.}, 442 U.S. 735, 740 (1979).
\item \textsuperscript{86} \textit{Bond v. U.S.}, 529 U.S. 334, 369 (2000).
\item \textsuperscript{87} \textit{Terry v. Ohio}, 392 U.S. 1, 17-18 (1968).
\item \textsuperscript{88} \textit{Harris v. U.S.}, 390 U.S. 234, 236 (1968).
\item \textsuperscript{89} \textit{Smith}, 442 U.S. at 742 (asserting that individuals could not have a subjective expectation of privacy in the numbers they dial when using a telephone, since all telephone users must realize that they must convey such numbers to the telephone company in order to complete a call).
\item \textsuperscript{90} Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997).
\item \textsuperscript{91} \textit{Oliver v. U.S.}, 466 U.S. 170, 178 (1984).
\end{itemize}
strated a subjective expectation.\textsuperscript{92}

1. \textit{Subjective Expectations In Thermal Imaging Technology}

While somewhat distant from the implications of face recognition technology, the thermal imaging technology used by police to detect the indoor growth of marijuana has provided some helpful insight in how courts could assess whether an individual has a subjective expectation of privacy. Two federal circuit courts have employed somewhat contrasting inquiries whether an individual has taken sufficient steps to conceal indoor marijuana growth.\textsuperscript{93}

Under the 'Waste Heat' analysis employed by the Eleventh Circuit Court of Appeals, inquiries are made into whether the individual made any attempt to conceal, or show concern for the resulting heat emissions from the lamps used to grow marijuana indoors.\textsuperscript{94} In contrast, the 'balance of the evidence' approach conducted by the Fifth Circuit Court of Appeals, is a broader inquiry and balances an individual's total actions against the excess heat emitted.\textsuperscript{95}

Under the Fifth Circuit's 'balance of the evidence' inquiry, the total conduct of an individual is assessed in determining whether they have demonstrated a subject expectation of privacy.\textsuperscript{96} In \textit{Ishmael}, thermal imaging disclosed a structure used to grow marijuana on defendant's rural property.\textsuperscript{97} While great care was taken to conceal its construction, both thermal imaging and utility records showed the building produced a lot of heat.\textsuperscript{98} A later search uncovered 770 marijuana plants.\textsuperscript{99} The trial court granted defendant's motion to suppress evidence, holding the thermal scan infringed upon his subjective expectation of privacy.\textsuperscript{100}

The Fifth Circuit addressed how to assess whether someone exhibits a subjective expectation of privacy.\textsuperscript{101} The court asserted that people do not have to take every precaution to exhibit such an expectation.\textsuperscript{102} Thus, the court used a 'balance of the evidence' approach, which measures whether a sufficient attempt is made to conceal indoor marijuana growth.\textsuperscript{103} In applying the test, the court asserted that defendant made

\textsuperscript{92} Bond, 529 U.S. at 1465.
\textsuperscript{93} Robinson \textit{v.} U.S., 62 F.3d 1325, 1328 n. 4 (11th Cir. 1995).
\textsuperscript{94} Id. at 1329.
\textsuperscript{95} \textit{U.S. v. Ishmael}, 48 F.3d 850, 854 (5th Cir. 1995).
\textsuperscript{96} Id.
\textsuperscript{97} Id. at 851.
\textsuperscript{98} Id. at 851-52.
\textsuperscript{99} Id. at 852.
\textsuperscript{100} Id. at 853.
\textsuperscript{101} Id. at 854.
\textsuperscript{102} Id.
a reasonable attempt to conceal the building's construction and chose to build in a rural locale. Such conduct outweighed defendant's inability to reduce the heat emissions. Thus, the court held that defendant exhibited a subjective expectation of privacy.

In comparison with the Fifth Circuit's method of assessing whether an individual has a subjective expectation of privacy, the Eleventh Circuit inquires in whether affirmative steps are made to conceal heat emissions coming from indoor marijuana growth. In Robinson, the police use of a thermal imaging device showed a large heat signature coming from defendant's home. Utility records revealed above average energy use, and defendant had recently bought sodium lamps and hydroponic equipment. A search showed a major indoor marijuana growing operation. At trial, defendant moved to suppress the seized marijuana, arguing that thermal imaging was illegal. The issue before the Eleventh Circuit was whether defendant had exhibited a subjective expectation of privacy. The court dismissed the 'balance of the evidence' approach employed by the Fifth Circuit, and instead applied a 'waste heat' analysis. Under this inquiry, the court determines whether the defendant attempted to reduce heat emission or demonstrate a concern for it. Here, the court noted that Defendant failed to take any affirmative steps to prevent or reduce the resulting heat, which showed a general lack of concern. Thus, in affirming the district court, the Eleventh Circuit held that the defendant did not exhibit a subjective expectation of privacy.

Therefore, both the Fifth and Eleventh Circuits employ somewhat different inquiries when assessing whether an individual has taken sufficient steps to demonstrate a subjective expectation of privacy. While the 'waste heat' analysis looks specifically on whether affirmative steps are taken to conceal heat emissions, the 'balance of the evidence' approach looks broadly at the total actions made in concealing indoor mari-
2. Subjective Expectations in Video Surveillance

When looking at what activities demonstrate such expectation with the potential for police naked-eye surveillance, the use of a ten-foot fence to shield an individual’s domestic agricultural interests has been deemed sufficient. When assessing the constitutionality of silent video surveillance, courts are extremely cautious in assessing how such surveillance took place, and the nature of the government intrusion. In looking at hidden video surveillance, some courts have looked towards specific activities like the closing of doors, the drawing of blinds, and the exercising of control over a private hotel room, in finding that an individual showed a subjective expectation of privacy. In addition, court outcomes are particularly fact driven, and outcomes often vary as to the specific fact pattern. Courts have measured the methods and duration of the video surveillance and the individual steps taken to protect his or her privacy.

In assessing whether an individual demonstrates a subjective expectation of privacy towards video surveillance, courts look to whether the individual voluntarily exposes his or her activities to the public. In Bailey, the defendant had moved to suppress evidence involving a video tape recording of a storage locker that appeared to show the defendant re-packing marijuana. Defendant had rented the locker unit in a self-storage commercial facility and was one of many people who had access to the facility. While defendant had sole access to the individual locker, the facility was not locked, and was open to members of the general public. In addition, defendant had failed to close the door of the locker facility when conducting the alleged activities.

The issue on appeal before the Supreme Court of Delaware centered on whether the nature of defendant’s choice of facility demonstrated a subjective expectation of privacy. In looking at the nature of the facil-

118. See id.
119. Ciraolo, 476 U.S. at 211.
121. U.S. v. Nerber, 222 F.3d 597, 603 (9th Cir. 2000) (asserting that the use of a hidden surveillance camera in a hotel room violated defendants subjective expectation of privacy).
122. Vega-Rodriguez, 110 F.3d at 179-180.
124. Id.
125. Id. at *1.
126. Id. at * 3.
127. Id.
128. Id.
129. Id. at *2.
ity, the court found that while the commercial storage facility was not exactly public, the defendant did know that it was not private. Furthermore, the facility was full of similar lockers, and defendant's actions could not have shown a subjective expectation of privacy, since the defendant could not have known whether the facility owners had placed monitoring equipment in the area, or when other fellow renters or staff could have personally viewed defendant's actions. However, the court drew specific attention to the fact that defendant voluntarily exposed himself to the surveillance, since defendant failed to close the locker door before engaging in the alleged activities, and thus chose to show the locker's contents to the public. Thus, the court denied defendant's motion to suppress evidence.

B. Reasonable Expectations of Privacy with Sensory Enhanced Surveillance

The Supreme Court has consistently asserted that matters open to public observation are not protected by the Fourth Amendment. Furthermore, non-intrusive government methods that provide only limited information do not infringe upon society's reasonable expectations of privacy. While naked-eye observations from vantage points freely accessible to the public do not constitute a search, the use of vision enhancing technology that reveals 'intimate details' does require a warrant under the Fourth Amendment.

1. Naked-Eye Aerial Surveillance

Government use of aerial naked-eye observations do not infringe upon society's expectation of privacy, as long as they are not constant. In California v. Ciraolo, Santa Clara police secured a private airplane and flew it over the respondent's home at an altitude of 1,000 feet within navigable airspace. From this overhead vantage point, officers trained in marijuana identification easily observed marijuana plants growing in the yard, which they photographed with a standard 35mm

130. Id. at *3.
131. Id.
132. Id.
133. Id. at *4.
135. U.S. v. Place, 462 U.S. 696, 707 (1983) (holding that a 'canine sniff' of defendant's luggage revealing narcotics failed to constitute a search under the Fourth Amendment since the method failed to expose luggage contents and afforded only limited information).
137. Ciraolo, 476 U.S. at 211.
138. Id. at 209.
camera. On appeal before the Supreme Court, the issue was whether the use of aerial photography violated society's reasonable expectation of privacy.

In looking at whether aerial observations infringe upon both personal and social values, the Court noted that the Fourth amendment protects the intimate activity associated with the sanctity of a man's home. However, any observation from a public vantage point, where a police officer has the right to be, which activities are clearly visible, does not offend the Fourth Amendment. Thus, because any individual flying in public airspace could observe the respondent's marijuana activities, the Court concluded that the police actions failed to offend society's reasonable expectation of privacy.

2. Vision Enhanced Aerial Surveillance

In addition to naked-eye aerial observations, vision-enhancing technology that does not reveal 'intimate details' also fails to violate society's reasonable expectation of privacy. In Dow Chemical, the Environmental Protection Agency ("EPA") used an aerial photographer to take precision photographs of petitioner's plant. The district court held the photographs infringed on petitioner's reasonable expectation of privacy. However, the Sixth Circuit reversed, asserting such government methods were similar to naked-eye observations, and thus did not require a warrant under the Fourth Amendment. The issue before the Supreme Court was whether the government use of vision enhancing surveillance technology offends society's reasonable expectation of privacy.

In recognizing that naked-eye observations do not require a warrant, the Court extended this reasoning to include technology that does not penetrate walls or windows. The Supreme Court noted that under the Fourth Amendment that the owner of commercial property enjoys a

---

139. Id.
140. Id. at 211.
141. Id. at 213.
142. Id. at 217.
143. Id. at 214–15.
145. Id. at 229. The "EPA employed a commercial aerial photographer, using a standard floor-mounted precision aerial mapping camera, to take photographs of [Dow Chemical's 2,000-acre facility in Midland Michigan]." Id. While the photographs were taken "from altitudes of 12,000, 3,000, and 1,200 feet," the EPA aircraft took the photographs within navigable airspace. Id.
146. Id. at 231.
147. Id.
148. Id. at 235.
149. Id. at 239.
diminished expectation of privacy, compared to the expectation of a homeowner.\textsuperscript{150} While the government conceded that the use of highly sophisticated surveillance techniques, not available to the public, could require a warrant, the court reasoned that the use of map-making photography failed to reveal ‘intimate details’ of Dow’s plant.\textsuperscript{151} Thus, government use of vision enhancing technology was acceptable under the Fourth Amendment, as long as it did not reveal specific information of activities within private property.\textsuperscript{152} Thus, the Court held that the EPA’s use of vision enhancing photography did not violate society’s reasonable expectation of privacy.\textsuperscript{153}

3. Secret Video Surveillance

While individuals have no legitimate expectation of privacy to be free from occasional ‘snooping’ like aerial observations, courts have asserted that society deems constant video surveillance of an individual’s home as unreasonable under the Fourth Amendment.\textsuperscript{154} When assessing whether video surveillance offends society’s reasonable expectation of privacy, the extent of that expectation often turns on the nature of the intended governmental intrusion.\textsuperscript{155} The Ninth Circuit has asserted that individuals do have an expectation of privacy against being videotaped in certain instances.\textsuperscript{156} Specifically, people may create temporary zones of privacy within which they may not be videotaped, even when the zone is a locale they do not own or control.\textsuperscript{157} Often, because images of an ‘Orwellian state’ are invoked with the use of hidden video surveillance, courts require the government provide a showing of necessity in order to justify its use.\textsuperscript{158}

Individuals have a reasonable expectation of privacy to be free of secret hidden video surveillance, even when the observation was brief in nature.\textsuperscript{159} In United States v. Nerber, the defendants entered a La Quinta Inn in Seattle to conduct a narcotics transaction with FBI informants.\textsuperscript{160} The FBI and local authorities had rented the room, installed hidden video cameras without first obtaining a warrant, and recorded the transactions with defendants.\textsuperscript{161} At trial, the defendants moved to

\begin{itemize}
\item \textsuperscript{150} Id. at 238.
\item \textsuperscript{151} Id.
\item \textsuperscript{152} Id.
\item \textsuperscript{153} Id.
\item \textsuperscript{154} U.S. v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987).
\item \textsuperscript{155} Id. at 251.
\item \textsuperscript{156} U.S. v. Teketa, 923 F.2d 665, 676-77 (9th Cir. 1991).
\item \textsuperscript{157} Id. at 677.
\item \textsuperscript{158} U.S. v. Torres, 751 F.2d 875, 882 (7th Cir. 1984).
\item \textsuperscript{159} Nerber, 222 F.3d. at 600.
\item \textsuperscript{160} Id. at 599.
\item \textsuperscript{161} Id.
\end{itemize}
suppress the evidence obtained from the video surveillance, which was granted. On appeal before the Ninth Circuit, the issue centered on whether such surveillance was reasonable under the Fourth Amendment.

The Ninth Circuit noted that the idea of a brief commercial transaction taking place in a short amount of time with lack of any previous connection between parties makes the issue of reasonableness a very close call. In assessing society's expectation of privacy, the court assessed the government's intrusion in implementing hidden video surveillance. Unlike aerial surveillance that is a one-time observation, the use of cameras are different since they allow all activities within view to be constantly recorded. However, in looking at the nature of the government's intrusion, the Ninth circuit agreed with the district court that defendants failed to have an expectation of privacy which society would deem as reasonable.

Defendant's expectation of privacy was greatly diminished because they were not 'residents' of the hotel where the transactions took place, nor were they overnight guests of the hotel. While defendants had an objective expectation of privacy when alone in a hotel room, such expectation was reduced when the activity was for the limited purpose of conducting a commercial transaction. Thus, the Ninth Circuit upheld the district courts denial of defendant's motion to suppress evidence.

IV. APPLYING CONSTITUTIONAL PRINCIPLES TO FACE RECOGNITION TECHNOLOGY

Because no federal or state court has directly analyze the constitutionality of face recognition technology, a court would likely have to assess the Fourth Amendment implications of such a government method

162. Id.
163. Id.
164. Id. at 600. The Nerber court focused on the Supreme Court's reasoning in Minn. v. Carter, in assessing reasonableness. Id. In Carter, defendants had entered a person's apartment for a brief period to conduct a narcotics transaction. Minn. v. Carter, 525 U.S. 83, 85 (1998). A police officer was able to peer through the window of a ground floor apartment, though a gap in the blinds, to observe the placement of white powder in bags. Id. The Supreme Court asserted that due to the purely commercial nature of the transaction, the short period of time on the premise, and the lack of connection with the parties, the officer's visual observations failed to violate society's reasonable expectation of privacy. Id. at 91.
165. Nerber, 222 F.3d at 602.
166. Id.; Cuevas-Sanchez, 821 F.2d at 251.
167. Nerber, 222 F.3d at 604.
168. Id.
169. Id. at 605.
170. Id. at 606.
FACE RECOGNITION TECHNOLOGY

under the *Katz v. United States* reasoning.\(^{171}\) First, a court would look at whether an individual's specific actions when being viewed and identified with face recognition technology demonstrated a subjective expectation of privacy.\(^{172}\) Second, the court would have to assess whether society regards identification through such methods as being reasonable.\(^{173}\) In assessing facial recognition technology under this framework, a court would look at the intrusive nature of such a search; whether the search fit more like a frisk or body search found in *Terry v. Ohio*, \(^{174}\) or whether it would be more like a non-physical 'canine sniff' as decided in *United States v. Place*.\(^{175}\)

A. DEMONSTRATING A SUBJECTIVE EXPECTATION OF PRIVACY IN FACE RECOGNITION IDENTIFICATION

While it would be difficult for an individual to show a subjective expectation of privacy in his or her face, an individual's conduct could show some steps to help preserve their facial features and activities as private.\(^{176}\) Just as courts have looked to specific factors in assessing such a subjective expectation, courts could look at each unique use of facial recognition technology, like in the context of a check-in at an airport, or at a public venue like the entertainment district of Ybor City, to assess the different nature of the use, and whether such a use would deserve heightened protection from the government intrusion.

1. Possible Factors of a Total Conduct Test

One possible approach would be to apply the Fifth Circuit's 'total conduct' test used in *Ishmael v. United States* in the face recognition context.\(^{177}\) Certainly, individuals must often enter public venues such as shopping areas, or grocery stores, in order to purchase and maintain their daily needs. Thus, it would almost be impossible for an individual to avoid public venues, in order to reduce the chance that their facial profile could be extracted and used for identification with face recognition technology. The Fifth Circuit was clear that when assessing whether an individual has a subjective expectation of privacy, an individ-

\(^{171}\) 389 U.S. at 360 (Harlan, J. concurring).

\(^{172}\) Id. at 361.

\(^{173}\) Id.

\(^{174}\) 392 U.S. at 17–18 (holding that due to the intrusive character and physical nature of a body search over an individual's clothing, that such a frisk constituted a search under the Fourth Amendment).

\(^{175}\) 462 U.S. at 707 (asserting that the use of a dog sniff to detect narcotics in concealed luggage failed to constitute a search under the Fourth Amendment due to the non-intrusive nature of the search).

\(^{176}\) *Smith*, 442 U.S. at 740.

\(^{177}\) *Ishmael*, 48 F.3d at 854.
ual does not have to take every precaution in order to exhibit such an expectation.\textsuperscript{178} Thus, when an individual has made any sufficient attempt to conceal their facial features, or attempted to avoid identification from facial recognition technology, such actions could be sufficient to show an expectation of privacy.\textsuperscript{179}

Celebrities and well-known music performers have often been known to wear wigs or don large sunglasses, in order to conceal their identities from the public. Certain religions and ethnic traditions require the use of certain headdresses, as recently seen by the numerous television reports on the traditional wearing of the burka by Afgan women. Thus, under the ‘total conduct’ test outlined by the Fifth Circuit, an individual donning some method of concealing their distinct facial identity to ward against identification using facial recognition technology could warrant a finding that that person has demonstrated a subjective expectation of privacy.\textsuperscript{180}

2. Possible Inquiry under an ‘Affirmative Steps’ Test

A second approach, slightly different from the \textit{Ishmael} inquiry, would be to assess under Eleventh Circuit reasoning whether an individual’s action of going out in public constitutes an ‘affirmative step’ sufficient to destroy any subjective expectation of privacy in his or her facial features.\textsuperscript{181} Under this more narrow inquiry, a court would look at whether an individual sought to prevent detection under face recognition surveillance, or if such an individual showed a general concern for such surveillance.\textsuperscript{182} Any activity in which an individual would avail himself or herself to face recognition technology, like entering a public sporting venue to attend a professional football game, could constitute ‘affirmative steps’ to reduce their subjective expectation of privacy.\textsuperscript{183} However, several actions could be performed by an individual to show concern for the possibility of being identified at such a sporting event.\textsuperscript{184} Apart from an individual donning the traditional ‘dog pound’ paraphernalia worn by Cleveland Browns fans, an individual could refrain from certain public locations within the stadium like the beer stand.\textsuperscript{185} Again, just as in the total conduct analysis, the wearing of certain items to alter their identity

\textsuperscript{178} Id.
\textsuperscript{179} See id.
\textsuperscript{180} See id.
\textsuperscript{181} Robinson, 62 F.3d at 1329.
\textsuperscript{182} Id.
\textsuperscript{183} See id. (describing application of the “affirmative step” test to the factual scenario).
\textsuperscript{184} See id. (analyzing how an individual’s actions can establish a subjective concern for privacy).
\textsuperscript{185} Id.; see \textit{Ishmael}, 48 F.3d at 854 (outlining how to assess an individual’s demonstration of a subjective expectation of privacy).
FACE RECOGNITION TECHNOLOGY

would help support a finding that an individual evidenced a subjective expectation under the Eleventh Circuit's reasoning.\footnote{Id.}

Thus, under the inquiry, wearing items like hats or glasses could mitigate against an individual's need to go into a public place where face recognition technology was used.\footnote{See id. (applying the court's reasoning in its assessment of a subject's conduct when evaluating demonstration of a subjective expectation of privacy).}

B. EXAMPLE OF TAMPA SUPER BOWL

A surveillance technique that is not generally known or understood often creates a situation where individuals could not have a subjective expectation of privacy.\footnote{See Smith, 442 U.S. at 740 (describing how the public's understanding of telephone technology impacts one's ability to demonstrate a subjective expectation of privacy); see also Ishmael, 48 F.3d at 854 (outlining the implications of thermal imaging techniques upon an individual's subjective expectation of privacy).} Both the ACLU and the Tampa area press were quick to point out that spectators at the 2001 Super Bowl were not aware, and were not told, that facial recognition technology was going to be used to scan the crowd to identify potential terrorists and wanted criminals.\footnote{Carey, supra n. 42, at ¶ 2.} Again, the central inquiry in assessing a subjective expectation of privacy is the person's state of mind.\footnote{Carey, supra n. 42, at ¶ 2.} The Tampa Super Bowl is a clear example of a situation where spectators could not have possibly demonstrated the requisite actions in order to manifest a subjective expectation of privacy, because they completely lacked the knowledge of the actual use of facial recognition technology.\footnote{See Vega-Rodriquez, 110 F.3d at 178 (describing the analysis of one's state of mind and its impact upon subjective expectation of privacy).} However, when the use of facial recognition technology at a location is well known and documented,\footnote{See id.} such as the use at Tampa's Ybor City entertainment district, such implementation would afford a more difficult inquiry.\footnote{Tampa Puts Face-Recognition, supra n. 23.} While the 2001 Super Bowl became one of the first well known uses of facial recognition technology, and although the technology has been pervasive in the media after the tragedy of September 11th, courts will have to look at whether the public was properly notified as to the use of the technology.\footnote{See Vega, 110 F.3d at 178 (discussing the state of mind of the subject as relevant to an assessment of the subjective expectation of privacy); see Smith, 442 U.S. at 740 (reviewing analysis of the subjective expectation of privacy).}
C. Assessing Whether Facial Recognition Technology is a Government Method Society Deems as Reasonable

When assessing whether a method of government surveillance constitutes a search, the Supreme Court of the United States has asserted that matters open to the public are not protected by the Fourth Amendment.\(^\text{195}\) Certainly, many of the actions associated with identification through facial recognition technology would be considered as matters open to the public, in that they occur within larger public venues such as airports, sporting events and entertainment districts. In addition, like other non-intrusive government methods like the canine sniffs used to detect drugs in airport luggage, facial recognition technology only intrudes upon the outward facial features that are exposed to the public.\(^\text{196}\) The documented uses of facial recognition technology have all been conducted from vantage points that are freely accessible to the public.\(^\text{197}\) While under these traditional inquiries into whether the government method would not infringe upon society's reasonable expectation appears to favor extending such principles to facial recognition technology, both the 'intimate details' analysis\(^\text{198}\) and case law directly addressing video surveillance\(^\text{199}\) could complicate the inquiry.

1. Reasonableness Under the 'Intimate Details' Analysis

The use of vision-enhancing technology that reveals 'intimate details' is not a government method which society would deem as reasonable.\(^\text{200}\) In addressing whether the use of map-making aerial technology constituted a search under the Fourth Amendment, the *Dow Chemical* court was particularly careful in pointing out that the use of highly sophisticated surveillance techniques, not available to the public, could potentially be deemed as unreasonable.\(^\text{201}\) Certainly, the actual taking of an individuals photographic likeness failed to constitute an 'intimate detail' under the *Dow Chemical* reasoning, since such an image could be viewed through naked-eye observations without the aid of technology.\(^\text{202}\)

However, the type of information obtained via facial-recognition technology could be deemed as 'intimate details.'\(^\text{203}\) With face-recognition technology, the software could potentially record both the time and

---

\(^{195}\) *Bond*, 529 U.S. at 336; see *Ciraolo*, 476 U.S. at 211.

\(^{196}\) *Place*, 462 U.S. at 707.

\(^{197}\) See *Ciraolo*, 476 U.S. at 211.

\(^{198}\) *Dow Chem.*, 476 U.S. at 239.

\(^{199}\) *Nerber*, 222 F.3d. at 600.

\(^{200}\) *Dow Chem.*, 476 U.S. at 239.

\(^{201}\) See id. at 238.

\(^{202}\) Id. at 239.

\(^{203}\) Id.
location a particular person was identified.\textsuperscript{204} For example, software could record that a person was located entering the Ybor City entertainment district at 9:05 p.m., who then entered a specific restaurant at 9:45 p.m., and then dined with another identified person starting at 10:00 p.m. Thus, while the actual extraction of that individuals' face in a public place would constitute a naked-eye observation, the total information obtained with the technology mirrors the 'Orwellian society' commentators fear with face recognition systems.

In addition to the specific details obtained from entering a single area that employed the facial recognition technology, if systems were networked, they could create more sweeping arrays of 'intimate details.'\textsuperscript{205} In expanding on the example provided above, a networked system could identify an individual in one location on a specific date, and identify that same person at a different location afterwards. A person recorded as entering Ybor City three days ago, could then be recorded at a Las Vegas gambling casino today, and then recorded as taking a flight to New York tomorrow. Certainly, a networked system recording could easily record these instances of identification to provide an accurate view of that person's public activities.

Both of these examples illustrate the potential of how face recognition technology could impact society and how such use when placed in this context probes into the 'intimate details' of an individual's life.\textsuperscript{206} Further, these examples illustrate exactly what the Supreme Court feared, that advancing technology could create the potential for a method that is clearly unreasonable, and would require a warrant under the Fourth Amendment.\textsuperscript{207} The single use of face recognition technology to scan a public venue to identify a potential terrorist or wanted criminal, may not actually arise to the level of 'Orwellian' proportions. However, as illustrated, the method does have this potential.

2. \textit{Reasonableness Under Video Surveillance Reasoning}

Unlike aerial surveillance, which only allows one-time observations, the proposed implementation of face recognition technology in public venues like airports would allow activities within such facilities to be constantly recorded.\textsuperscript{208} Just like with video surveillance, courts could assert that in facilities that use face recognition identification of employees or visitors, such individuals should be afforded certain zones of pri-

\textsuperscript{204} Jane Black, \textit{FaceIT, Face-Cams are Here to Stay} ¶ 3 <http://businessweek.com/bwdaily/dnflash/nov2001/nf20011115_3919.htm> (accessed Apr. 22, 2002).
\textsuperscript{205} \textit{Dow Chem.}, 476 U.S. at 239.
\textsuperscript{206} Id.
\textsuperscript{207} Id.
\textsuperscript{208} \textit{See Cuevas-Sanchez}, 821 F.2d at 251.
Thus, a court in assessing the reasonableness of facial recognition technology would have to compare such methods along the same lines as video surveillance and assess the nature of the government intrusion.\textsuperscript{210}

As provided by the \textit{Nerber} reasoning, courts in assessing whether video surveillance constitutes an unreasonable intrusion should look to where the activities take place and the purpose of the individual’s conduct.\textsuperscript{211} In areas where individuals go for the limited purpose of conducting commercial transactions, courts view the hidden video surveillance of such activities as having a heightened level of intrusiveness.\textsuperscript{212} Certainly the areas where face recognition technology could potentially be implemented, such as airports and entertainment centers, are locations where individuals go simply for a short period of time in order to conduct a consumer transaction.\textsuperscript{213} Thus, unlike a home, which is afforded the highest level of Fourth Amendment protection, a court in assessing the intrusiveness of such public surveillance could potentially view it as unreasonable.\textsuperscript{214}

Lastly, the potential exists that, in time, society could regard the use of face recognition technology as reasonable. Just as society over the last twenty years has simply become use to the idea of being the object of video surveillance at shopping malls, convenience stores, and banks, society could get use to similar observation implementing face recognition technology.\textsuperscript{215} Society’s views and norms have always changed and adapted over time, and society could quickly acquiesce to the use of this technology. In addition, with society’s fears of potential terrorist takeover of domestic commercial flights after September 11\textsuperscript{th}, society could immediately view face recognition technology as an acceptable privacy invasion. Thus, like with certain types of video surveillance, face recognition technology could be deemed today as an invasion which society deems as reasonable, and thus not a search under the Fourth Amendment.

V. CONCLUSION

After the tragic events of September 11\textsuperscript{th}, and the need for added security in our nation’s airports and public venues, face recognition technology will continue to be researched, advanced, and implemented. Al-

\textsuperscript{209} Teketa, 923 F.2d at 677.
\textsuperscript{210} Id.
\textsuperscript{211} Nerber, 222 F.3d at 603.
\textsuperscript{212} Id.
\textsuperscript{213} See id.
\textsuperscript{214} See id.
\textsuperscript{215} Burrows, supra n. 10, at 1079.
though the use of this technology has not been sufficiently proven in venues like Tampa's Ybor City and the hockey arena of the Salt Lake City Winter Olympics, corporations like Visionics and Viisage persist on developing and implementing these systems. While these systems may not accurately or effectively identify potential terrorists or criminals at our nation's airports, they still may have the potential to deter such individuals from entertaining ideas of hijacking a commercial aircraft. However, the fact remains that no face recognition system has ever led to the actual identification and arrest of a criminal or terrorist.

The constitutional issues of facial recognition technology remain unresolved. However, if and when the constitutionality of such a system is brought to court, both Katz inquiries would have to be addressed in assessing if the technology constitutes a search under the Fourth Amendment. As a fact intensive inquiry, it is possible that an individual could demonstrate a subjective expectation of privacy. Certainly, an individual's affirmative steps to conceal their identity, such as wearing a hat or sunglasses, could be sufficient to demonstrate such an expectation. Furthermore, individuals by simply going to a public facility like a grocery store or shopping mall, have not necessarily shown sufficient steps to be deemed to have a lower expectation or privacy. Rather, courts would have to assess an individual's total conduct in assessing whether his or her state of mind demonstrated a sufficient expectation of privacy. However, the more fundamental question becomes whether people will begin to alter how they look when entering facilities that use face recognition technology.

In addition, whether society would deem the use of this technology as reasonable may depend upon how it is implemented, as well as what society's willingness to accept privacy reducing methods following September 11th. Certainly, the immediate public reaction following the tragic events in New York and Washington was to implement any technology in domestic airports to alleviate long lines, and to identify any individuals with known ties to terrorist groups. Thus, society may already regard face recognition technology as a reasonable expectation of

216. MacMillan, supra n. 47, at ¶ 16.
217. Id.
218. Stanley, supra n. 37, at ¶ 14.
219. 389 U.S. at 360.
220. Ishmael, 48 F.3d at 854.
221. Id.
222. Id.
223. Id.
224. Leonard, supra n. 6, at ¶ 4.
225. O'Harrow, supra n. 7, at ¶ 1.
privacy. However, only time will tell if society’s perspective will revert to a more privacy wary mentality.

Apart from society’s perspective in light of September 11th, certain aspects of face recognition technology could provide the level of ‘intimate details’ to be far too intrusive to constitute a reasonable expectation of privacy. The potential for the technology to allow the government to know the day-to-day activities of public citizens does create the potential for an “Orwellian” state. While the public has become acclimated to regular video surveillance at public venues like banks, grocery stores, and shopping malls, society would not tolerate the ability of the government to obtain such detailed and specific information. Under this context, such a method should be deemed as overly intrusive, and thus a search under the Fourth Amendment.

It should be noted that while facial recognition has not been effectively implemented and while the aforementioned reasoning appears to cast a dark shadow on whether such a system violates an individual’s legitimate expectation of privacy, the technology does have the potential to be something which is both useful and needed in this country. Face recognition technology does have the potential to ease the fears of airline travelers, and help reduce the chance for a repeat performance of September 11th. Similar biometric technologies implemented overseas in international airports demonstrate a real need to implement similar precautions in domestic airports as an increased security measure to avoid future terrorists plots. Thus, the potential for such systems to accurately identify individuals could increase the value of such methods, and therefore help balance against their privacy implications.

Therefore, only through the continued evaluation and criticism of face recognition technology by privacy advocates and other commentators will there be assurances that the method will not offend the policies underlying the Fourth Amendment. With no case law and no federal legislation in place, peripheral technologies like video surveillance and thermal imaging will allow constructs to evaluate the constitutionality of face recognition technology.

Robert H. Thornburg†

---

227. See Ishmael, 48 F.3d at 854.
228. Konrad, supra n. 21, at ¶ 2.
229. Vonderheid, supra n. 74, at ¶ 6.

† J.D. Candidate December 2002, University of Florida Levin College of Law, B.S. in Chemical Engineering, cum laude, University of Notre Dame.