NOTE

CAN CORPORATE AMERICA SECURE OUR NATION? AN ANALYSIS OF THE IDENTIX FRAMEWORK FOR THE REGULATION AND USE OF FACIAL RECOGNITION TECHNOLOGY

David McCormack[*]

---

[*] J.D. Candidate, Boston University School of Law, 2003; B.S., Providence College, 2000.

I. INTRODUCTION

In an eerily prophetic letter dated June 18, 2001, William Wilson, the chairman of the International Biometric[1] Industry Association, warned the California legislature that restricting the use of facial recognition technology could result in the inability of law enforcement to stop a terrorist airline attack by the associates of Osama Bin Laden.[2] Wilson urged the legislature to reconsider its bill limiting the use of this technology so that the full value of facial recognition technology could be utilized, making the public safe and secure from such a terrorist threat.[3] On September 11, 2001, Wilson's worst fears were realized in New York City and Washington, D.C., and the controversy regarding the use of facial recognition technology was born anew with a sudden urgency.

Used primarily as a crime deterrent in large cities, many now bill facial recognition technology as a solution to the U.S. airport security crisis.[4] Other nations have already taken advantage of the abilities of facial recognition technology, implementing the system in their own airports. The U.S. had been slow to warm to facial recognition technology because of public concern for fundamental privacy rights.[5] The events of September 11, 2001 have since quelled the public's apprehension, and the technology they once vilified as an

---

[1] Biometrics is an electronic code based on the unique features of an individual that may provide an effective and secure barrier against unauthorized access to information and secure areas. *See Understanding Biometrics*, *at* Visionics.com, http://www.visionics.com/newsroom/biometrics (Mar. 21, 2002).

[2] *See Letter Regarding CA Legislation*, *at* IBIA.org, http://www.ibia.org/calegletter061801.htm (Jun. 18, 2001).

[3] *See id.*

[4] Richard Richtmyer, *Air Security Tech Eyed*, CNNFN.COM, *available at* http://www.cnnfn.com/2001/09/13/technology/airport_tech/index.htm (last visited Oct. 30, 2001).

[5] *Id.* (noting that the U.S. company Identix has installed its facial recognition system at an airport in Keflavik, Iceland, and will install another system at Heathrow Airport in London).

invasion of privacy, they call upon to protect them and to provide a face and an identity to terrorism.[6]

Despite this call for protection, the government and private industry currently provide no procedural safeguards or regulations that ensure the proper use of the technology, and proposed regulations do not adequately address the situation.[7] City ordinances have loosely governed its use, while privacy groups and industry leaders have universally failed to secure assurances that law enforcement will not misuse the system.[8]

Due to the vast uncertainty regarding the use of this technology, the Identix Corporation, which manufacturers FaceIt facial recognition software, and is the worldwide leader in identification technologies and systems, announced a comprehensive framework for the employment of facial recognition technology in improving airport security.[9] Entitled *Protecting Civilization from the Faces of Terror: A Primer on the Role Facial Recognition Technology Can Play in Improving Airport Security* (*"Protecting Civilization")*, this "white paper" details five key areas where facial recognition technology could enhance airport security, while also addressing privacy concerns and the need for formal guidelines and procedures to protect against abuse of the system.[10] While the framework is skeletal, it represents a reasoned and thoughtful approach to realizing the benefits of facial recognition technology while protecting the privacy rights of those who are affected by it. As a non-legal framework created by a corporation who would financially benefit from the use of facial recognition technology, the "white paper" raises two issues: (1) is there a need for formal regulation or is industry self-regulation enough, and (2) is the framework thorough enough so that Congress can turn it into a comprehensive regulation?[11]

As our government moves to assure our safety, it needs to be mindful that rational, effective, and ethical use of facial recognition technology is necessary to protect our privacy and ensure that the technology is not abused by those

---

[6] Julia C. Martinez, *Face-ID Technology Gains New Support*, DENVER POST, Sept. 19, 2001, at A-1.

[7] Ivan Amato, *Big Brother Logs On*, TECHNOLOGY REVIEW.COM, *available at* http://technologyreview.com/articles/amato0901.asp (Sept. 2001).

[8] *Id.* (acknowledging the numerous unsuccessful attempts to introduce legislation aimed at protecting privacy and restricting the use of facial recognition technology).

[9] Identix Inc. Web site, *Visionics Corporation Announces Framework for Protecting Civilization from the Faces of Terror*, *available at* http://www.shareholder.com/identix/ReleaseDetail.cfm?ReleaseID=59253 (Sept. 24, 2001).

[10] *Protecting Civilization from the Faces of Terror: A Primer on the Role Facial Recognition Technology Can Play in Improving Airport Security* [hereinafter "Protecting Civilization"], *available at* http://www.eyeforetravel.com/papers.counterterrorism_wp_-_us.pdf (last visited Oct. 30, 2002).

[11] *Id.*

who are given the power to employ it. This Note proposes a method for incorporating the Identix framework into a system of regulations, safeguards, and penalties for the effective and legal use of facial recognition technology in airports and other areas of high national security. Part II will focus on the capacity of facial recognition technology to enhance the ability of law enforcement agents to detect and apprehend criminals, the evolution of the use of the technology in the U.S., and the technology's potential for abuse. Part III will discuss the legality of facial recognition technology by examining its relationship with the Constitution and federal and state law. Part IV will then discuss the shortcomings of self-regulation and the reasons why comprehensive regulation is needed. Finally, Part V will suggest ways in which legislators can complete the Identix framework to form a thorough and feasible standard for the use of facial recognition technology as a public security measure.

II. FACIAL RECOGNITION TECHNOLOGY AND ITS PRESENT USE

A. How Facial Recognition Technology Operates

To understand how law enforcement can use facial recognition technology as a form of public security, it is important to first understand how the system works. The Identix Corporation's FaceIt software automatically detects a human presence, locates and tracks faces, and extracts images from a video feed for identification by matching the extracted face against a pre-existing database of people.[12]

As presently used today to scan crowds in public areas, this technology begins with the extraction of a person's image by a video camera.[13] The image is run through the software and FaceIt then creates a digital map of the extracted face by translating the contours into mathematical formulas, creating an identification of a person similar to the unique characteristics of a fingerprint.[14]

Law enforcement officials subsequently run the digital face map against a database of suspected or known criminals, primarily through the use of digital mug shots that the user scans into the system.[15] A match results in a red flag and law enforcement officials monitoring the system notify others of the

---

[12] Identix Inc. Web site, *FaceIt: At a Distance, In a Crowd, At a Glance* [hereinafter "*FaceIt*"], *at* http://www.identix.com/newsroom/whatisfaceit.html (Last visited Oct. 30, 2002).

[13] *Id.*

[14] Robert O'Harrow, Jr., *Matching Faces with Mug Shots*, WASH. POST, Aug. 1, 2001, at A1.

[15] *Id.*

suspected or known criminal's presence in a given area.[16] The FaceIt system is capable of scanning almost 70 million images per minute on a standard 733-megahertz personal computer.[17]

Under the most favorable conditions, the error rate for a match is less than one percent.[18] While the software can generally take things such as changes in lighting, aging, and facial hair into account, FaceIt is not one hundred percent accurate and the precision of the process depends on the clarity of the photos in the database and the photos the video camera captures.[19] Manufacturers still recommend using a backup system despite the small possibility of a system error. They back up the system by utilizing other biometric technologies such as retinal recognition or fingerprint identification to ensure that correct results.[20]

B. Utilization of Facial Recognition Technology in Public Areas in the U.S. and Abroad

Although law enforcement authorities have used closed circuit surveillance systems for many years, it has only recently explored the capabilities of facial recognition technology.[21] Elsewhere, England was the first country to harness the power of facial recognition technology when it combined FaceIt with 300 surveillance cameras in a crime-riddled section of London in 1998.[22] Officials cited the software as the prime reason for a 34 percent drop in the crime rate and, as a result, England has similar initiatives currently underway in other high crime areas.[23] After initial public concern, the sharp reduction in crime left many residents with no choice but to embrace the technology.[24] In other

---

[16] Visionics Corp., *FaceIt Will Enhance & Compliment Your CCTV Surveillance System!*, *available at* http://www.metadata.com.mx/cctvsurv/pdf (last visited Oct. 30, 2002).

[17] Jay Lyman, *Critics Blast U.S. Ties to 'Snooper Bowl' Technology*, NEWSFACTOR.COM, *at* http://www.newsfactor.com/perl/story/12458.html (last visited Oct. 30, 2002).

[18] *See* O'Harrow, *supra* note 13 ("The accuracy . . . depends on the clarity of both the photos in a database and the images being captured and searched, so that gloomy conditions could lower the accuracy. Match rates also could fall if the face is recorded at an odd angle.").

[19] Julia Scheeres, *Smile, You're on Scan Camera*, WIRED, *available at* http://www.wired.com/news/technology/0,1282,42317-2,00.html (Sept. 17, 2001) (quoting biometrics expert Julian Ashbourn, "There are a number of variables to the real-life application of facial technology. It will never be 100 percent accurate.").

[20] *Id.* (quoting David Teitelman, CEO of biometric company eTrue: "Every biometric has its strengths and weaknesses. We recommend that our customers use at least two biometrics.").

[21] *See id.*

[22] O'Harrow, *supra* note 13.

[23] *Id.*

[24] Amato, *supra* note 6 (offering a London resident's written opinion, "I am prepared to

areas of the world, Israeli authorities have used FaceIt as a safety precaution in the Gaza strip, while Mexican and Ugandan officials have used the system's personal identification capabilities to effectively control voter registration and prevent voter fraud.[25]

Back in the U.S, some people have used facial recognition technology for years, including casinos looking for cheats, banks seeking to eliminate ATM thefts, and Departments of Motor Vehicles attempting to reduce forgery. The technology's use in public places to identify criminals, however, is a relatively new phenomenon in the U.S.[26]

The first public ire over facial recognition technology in this country surfaced when stadium officials at Super Bowl XXXV in Tampa, Florida photographed thousands of unsuspecting fans as they entered the stadium.[27] The resulting criticism led many to dub the event "The Snooper Bowl."[28] Checking the faces of 100,000 fans against a database of 1,700 criminals, the Viisage Corporation's FaceFINDER system registered 19 hits, only one of which monitors considered worthy of dispatching a police officer to investigate.[29]

Undeterred by the sharp criticism in the wake of the event, on June 29, 2001 Tampa officials began using Visionic's FaceIt software in the historic Ybor City entertainment district, where as many as 35,000 people stroll through each day.[30] Curbside signs reading "Area Under Video Monitoring" line the streets as people can see 36 surveillance cameras on tall poles every block or so.[31] Nearby, police officers monitor 10 video screens, looking for wanted criminals and missing children.[32]

Public outrage grew[33] and the situation drew national attention when House Majority Leader Dick Armey of Texas came forward denouncing the use of

---

exchange a small/negligible amount of privacy loss so I don't have to be caught up in yet another bomb blast/scare.").

[25] O'Harrow, *supra* note 13.

[26] *See* A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STAN. L. REV. 1461, 1478 (2000).

[27] Lyman, *supra* note 16.

[28] *Id.*

[29] Martin Kasindorf, *'Big Brother' Cameras on Watch for Criminals*, USA TODAY, *available at* http://www.usatoday.com/life/cyber/tech/2001-08-02-big-brother-cameras.htm (Aug. 2, 2001) (noting that the one investigation, of an alleged ticket scalper, did not result in arrest because the suspect fled from the scene).

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.* (stating that activists repeatedly marched through Ybor City chanting, "Big Bro, hell, no.").

facial recognition technology to spy on the public.[34] Despite the overwhelming public disapproval of the system, the City Council, in a 4-2 vote, decided that FaceIt was a preventive measure that effectively increased the safety of the public, and it rejected a motion to terminate the city's contract with Identix.[35]

The contrasting results in two other U.S. cities illustrate the polarity of views that exist concerning the use of facial recognition technology. Virginia Beach, Virginia has adopted a public facial recognition system similar to that of Tampa as a protective law enforcement tool,[36] but the Oakland, California City Council voted down a similar measure at the request of the city's Police Department.[37]

The Tampa experiment proved to be short-lived, however. Only six months after the controversy began with the use of the facial recognition technology system, privacy groups celebrated as it appeared that law enforcement officials had almost completely abandoned use of the system.[38] The American Civil Liberties Union ("ACLU") claims that the failure of the system to identify even a single individual in the database may have caused the downfall of the experiment.[39] Although the technology apparently failed in this situation, its use as a security measure to protect citizens by other means should not be dismissed.

---

[34] David McGuire, *Rep. Armey Blasts Tampa Over Face-Recognition System*, INFOWAR.COM, *at* http://www.infowar.com/class_1/01/Class1_070301a_j_shtml (July 2, 2001) (Rep. Armey argued that "[p]lacing police officers in a remote control booth to watch the every move of honest citizens isn't going to make us safer.").

[35] Robert MacMillan, *Tampa Face Recognition Vote Rattles Privacy Group*, NEWSBYTES, *available at* http://www.infowar.com/class_1/01/class1_08301a_j_shtml (Aug. 3, 2001).

[36] *Id.*; Electric Privacy Information Center, *Face Recognition*, [hereinafter "*Face Recognition*"] EPIC.ORG, *available at* http://www.epic.org/privacy/facerecognition (Jan. 17, 2002) (noting that the Virginia Department of Criminal Justice gave Virginia City a $150,000 grant in order to use facial recognition technology as a means of identifying suspected criminals and missing children).

[37] ACLU Press Release, *Oakland City Council Kills Video Surveillance Project: ACLU Cites Important Lessons for Other Cities*, ACLU.ORG, *at* http://www.aclunc.org/aclunews/news597/video.html?video (Sept. 22, 1997) (quoting Police Chief Joseph Samuels, Jr. as saying, "[C]oncerns about governmental intrusions and abridgment of civil liberties from residents and merchants of this city will likely negate the advantages and potential of this method of crime prevention.").

[38] ACLU Press Release, *Drawing a Blank: Tampa Police Records Reveal Poor Performance of Face-Recognition Technology*, ACLU.ORG, *at* http:// aclu.org.news/2001/n010302a.html (Jan. 16, 2002).

[39] *Id.* (remarking that although system logs indicate that the lack of positive identifications is true, Tampa police officials claim that the discontinuation is due to disruption caused by police redistricting and that they will resume the operation at some future point in time).

In the wake of September 11, law enforcement, public officials, and politicians began to explore new uses for facial recognition technology,[40] including exploring the ability of the technology to create a nationwide shield to scan airports and other areas of national security for terrorists and criminals.[41] Beginning in May 2002, Viisage Technology and Identix installed their software on a trial basis at Boston's Logan Airport, and while flaws in the system were evident, representatives of the companies proclaimed that the software detected suspects 90 percent of the time, and only once wrongly identified a person as a suspect.[42] This represented the first use of facial recognition technology for airport security in the U.S.[43]

C. Potential for Abuse

Critics of facial recognition technology point to the vast potential for abuse that the software presents. They argue that law enforcement's use of facial recognition technology could lead to the growth of a police state with military and national security agencies having greater involvement in the policing of U.S. citizens.[44] Authorities could misuse the technology to record intimate and private conduct.[45] Without regulation, law enforcement could use facial recognition technology for the discriminatory targeting of minorities and those with unfavorable political beliefs, tracking the whereabouts of individuals solely on the basis of race, religion or other characteristics.[46] Further, critics fear that law enforcement could share the information it collects by facial recognition technology with other government agencies for purposes other than national security.[47] Unfortunately, these Orwellian concerns are very real and illustrate the urgent need for the comprehensive regulation of facial recognition

---

[40] *See* Richtmyer, *supra* note 3.

[41] Robert O'Harrow Jr., *Facial Recognition System Considered for U.S. Airports*, WASHINGTONPOST.COM, *at* http://www.washingtonpost.com/ac2/wp-dyn/A14273-2001Sep23?language=printer (Sept. 24, 2001).

[42] Hiawatha Bray, *Reliability of Face-Scan Technology in Dispute*, BOSTON GLOBE, Aug. 5, 2002, at C1 (noting that the level of work to be performed by employees monitoring the system as it is currently used might make the system "too costly and difficult to run").

[43] Viisage in the News, *Viisage Selected to Deploy the First Face-Recognition Technology System for Security in a U.S. Airport*, VIISAGE.COM, *at* http://www.viisage.com/october_04_2001.htm (Oct. 15, 2001).

[44] Christopher Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 328 (1999).

[45] ACLU Press Release, *ACLU Calls on Law Enforcement to Support Privacy Laws for Public Video Surveillance*, ACLU.ORG, *at* http://www.aclu.org/news/1999/n040899b.html (Apr. 8, 1999).

[46] Milligan, *supra* note 43, at 328.

[47] *Id.* at 329 (noting that different organizations could easily cooperate to track an individual from place to place).

technology to ensure that individual rights will not be trivialized while the country improves its national security.

III. FACIAL RECOGNITION TECHNOLOGY AND THE LAW

As currently used, the Constitution, federal law, and state law do not appear to bar facial recognition technology for public security measure.[48] The reasoning behind this conclusion relies on an analysis of facial recognition technology in the context of the Supreme Court's jurisprudence in the areas of privacy rights, the Fourth and Fifth Amendments, and federal and state law. Thus far, the bulk of regulation concerning law enforcement's use of technologically-assisted surveillance derives from the courtroom, not the chambers of legislatures.[49]

A. Privacy as a Fundamental Right

Many commentators argue that facial recognition technology impinges on the right to privacy.[50] While the text of the Constitution does not specifically guarantee a right of privacy, the Supreme Court has recognized a limited right of privacy in a series of cases, including *Griswold v. Connecticut*,[51] *Roe v. Wade*,[52] and *Whalen v. Roe*.[53] This recognized right of privacy is drawn from zones of privacy or "penumbras" created by the First, Third, Fourth, Fifth, and Ninth Amendments.[54]

Although the right to privacy is without any explicit authority at the federal level, states have the power to create rights for their people beyond those present in the U.S. Constitution.[55] Several states have expressly afforded their citizens an individual right to privacy.[56] California has not only created privacy rights for its citizens in its constitution, it has also declared that privacy

---

[48] *See* Stephen Coleman, *Biometrics: Solving Cases of Mistaken Identity and More*, 69 FBI LAW ENFORCEMENT BULL. 6 (June 2000) (noting the legality of fingerprints could serve as a precedent for privacy challenges to facial recognition), *available at* http://wwwnesbary.com/class/621/articles/coleman.htm.

[49] Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J. L. & TECH, 383, 389 (1997).

[50] Amato, *supra* note 6; Froomkin, *supra* note 26, at 1478.

[51] 381 U.S. 479 (1965) (holding that the right of privacy encompasses the use of birth control measures).

[52] 410 U.S. 113 (1973) (holding that abortion is a fundamental, but not absolute, right).

[53] 429 U.S. 589 (1977) (holding that there is an interest in independence in making important personal decisions).

[54] *Griswold*, 381 U.S. at 484-85.

[55] Quentin Burrows, Note, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 VAL. U.L. REV. 1079, 1112 (1997).

[56] *Id.* at 1113-14 (identifying Pennsylvania, Oregon, Alaska, Hawaii, Montana, and California as states which explicitly provide an individual right to privacy).

is an inalienable right.[57] One cannot underestimate the role of state courts and legislatures in determining and expanding privacy rights concerning facial recognition technology because they may provide an appropriate guide for the development of modern privacy rights.[58] Any comprehensive federal law regulating the use of the technology would preempt these state-created privacy rights and therefore must also be analyzed.

B. Facial Recognition Technology in Public Areas and the Fourth Amendment

Assuming that limited rights to privacy exist on the state and federal level, facial recognition technology must also be examined against the Fourth Amendment to determine whether the technology's use implicates these rights, thus making its use as a security measure a "search" and rendering it unconstitutional absent a search warrant.[59]

1. Background Regarding Fourth Amendment Jurisprudence and Surveillance

As presently used, facial recognition technology is not generally implemented pursuant to a search warrant, although it could prove beneficial in environments where law enforcement officials do not have a warrant to conduct a search.[60] The question of its constitutionality is more likely to arise when used as a sense-enhancing law enforcement tool designed to randomly sweep and monitor public areas of high traffic or crime.[61]

Where law enforcement does not accompany its use of facial recognition technology with a search warrant, their actions must pass constitutional muster under the two-pronged test set out in *Katz v. United States*.[62] Justice Harlan, in

---

[57] CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life, liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

[58] Burrows, *supra* note 54, at 1111 (suggesting that a proposal to ban video surveillance may stem from state constitutional privacy rights expressed in a model statute).

[59] The Fourth Amendment states:

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

U.S. CONST. amend. IV.

[60] Milligan, *supra* note 43, at 318 (stating that the technology could be of possible benefit when used pursuant to a search warrant when law enforcement has not identified all of the suspects).

[61] *Id.* (noting possible public areas where law enforcement could use facial recognition technology includes airport terminals, border entry points, and housing projects).

[62] 389 U.S. 347 (1967).

his concurring opinion, elucidated the two-pronged test for determining whether a disputed warrantless law enforcement action is a search under the meaning of the Fourth Amendment.[63] In order for a police action to constitute a search, a person must have "exhibited an actual expectation of privacy," and this subjective expectation must be one that "society is prepared to recognize as reasonable."[64] While a person may enjoy a reasonable subjective expectation of privacy in his home, the Fourth Amendment does not protect objects, activities, or statements one reveals to the "plain view" of the public.[65]

The current Supreme Court employs Harlan's two-pronged test when determining the constitutionality of other forms of warrantless technologically assisted surveillance. In *Dow Chemical Co. v. United States*,[66] the Court ruled that Dow Chemical did not have a reasonable expectation of privacy from the taking of aerial photography in a navigable airspace by EPA enforcement officials.[67] Chief Justice Burger, writing for the majority, emphasized that the public's ability to engage in the activity at issue helps make Dow Chemical's expectation of privacy unreasonable.[68] The Court indicated that the use of more advanced surveillance equipment, not generally available to the public, might warrant Fourth Amendment protection.[69]

Recently, in *Kyllo v. United States*,[70] the Court tackled the issue of high-tech, sense-enhancing surveillance equipment, albeit in a ruling limited to surveillance of a defendant's home. The case involved the Department of the Interior's use of a thermal-imaging device on the defendant's home to detect the presence of high intensity lamps used to grow marijuana.[71] Based on evidence received from this scan and subsequent findings, a federal magistrate judge issued a search warrant to search the defendant's home, and police subsequently uncovered a marijuana-growing operation constituting more than 100 plants.[72]

To reach its conclusion on whether the thermal-imaging scan constituted a search, the Court attempted to confront "what limits there are upon [the] power

---

[63] *Id.* at 361.

[64] *Id.*

[65] *Id.*

[66] 476 U.S. 227 (1986).

[67] *Id.* at 238-239.

[68] *Id.* at 231, 239 (finding "any person with an airplane and an aerial camera could readily duplicate [the pictures]," and "[what] is observable by the pubic is observable without a warrant by government inspectors as well").

[69] *Id.* at 238 (acknowledging that even the Government conceded that the "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public . . . might be constitutionally proscribed absent a warrant.").

[70] 533 U.S. 27 (2001).

[71] *Id.* at 29-30.

[72] *Id.* at 30.

of technology to shrink the realm of guaranteed privacy."[73] Although purporting to confront this broad issue, the Court limited its holding by only prohibiting the use of sense-enhancing technology not available to the general public, to obtain any information regarding a home's interior that law enforcement could not be obtain absent a physical intrusion.[74] The Court's holding, although it involved a relatively crude sense-enhancing tool, was an attempt to protect against the ever-growing capabilities of sense-enhancing technology.[75]

2. The Constitutionality of Facial Recognition Technology Within the Meaning of the Fourth Amendment

Based on analogies drawn to these cases, it appears that the Supreme Court would not consider the use of facial recognition technology to scan airports and other public areas a search under the Fourth Amendment. Law enforcement, therefore, could have free reign to use it as a form of public surveillance.[76]

FaceIt and other facial recognition software use the image of a person's face, a feature that one knowingly displays to the public and, according to the *Katz* court, is beyond Fourth Amendment protection.[77] Specifically, a person cannot have a reasonable expectation to be free from a search of what one exposes to the plain view of the public.[78] On this basis, the discussion of the constitutionality of the use of facial recognition technology could end there.

Some assert, however, that facial recognition software actually captures images that are not exposed to the plain view of the public. These commentators argue that facial recognition technology does not simply capture the image of a person's face as a standard video camera does, but it instead creates a complex mathematical formula that can precisely identify an individual.[79] The logic would follow that while a person may have no reasonable expectation of privacy from having his image photographed, because he has not knowingly revealed the intricacies and contours of his face that the naked eye cannot view, he thus may claim a reasonable expectation of privacy from the use of facial recognition technology in public areas.[80]

---

[73] *Id.* at 34.

[74] *Id.*

[75] *Id.* at 36 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

[76] *Katz*, 389 U.S. at 361.

[77] *Id.*

[78] *Id.*

[79] *See* O'Harrow, *supra* note 13.

[80] *See Katz*, 389 U.S. at 361.

Such an argument fails because facial recognition technology only captures what a person knowingly exposes to the public.[81] The naked eye can see the contours and features of one's face, albeit on a lesser level to human detection than technologically-assisted detection. The escalation in the use of technologically assisted surveillance and its approval by the Supreme Court endorses this view, and suggests that the realm of what one knowingly exposes to the public grows as the technology capturing it is constitutionally approved.[82] In addition, facial recognition technology's present use involves widespread public notice of the system's capabilities and signage alerting the public that law enforcement is using the software in a given area so that a person is indeed aware of what he is exposing to the public.[83]

The *Kyllo* Court's concern about the accessibility of the technology to the public is not present in this context.[84] While *Kyllo* involved the use of an infrared thermal device available only to law enforcement agencies, any person can purchase FaceIt and other forms of facial recognition technology from the manufacturer, and it requires only a standard personal computer to run properly.[85] Since anyone can purchase a standard personal computer from a retailer and the software directly from a manufacturer, this distinction seemingly would lead the Supreme Court to uphold the technology's use by determining that it is akin to the aerial photographs in *Dow Chemical*.[86]

In the end, use of facial recognition technology would withstand judicial scrutiny under the Fourth Amendment, and, therefore, it would not implicate the limited rights of privacy the Supreme Court has created. The analysis does not end there, however, because use of facial recognition technology must also withstand judicial scrutiny against the Fifth Amendment's prohibition against self-incrimination.

C. Facial Recognition Technology in Public Areas and the Fifth Amendment

Although people generally invoke the Fifth Amendment in the classic courtroom setting, the introduction of high-tech biometric devices may allow people to invoke the Fifth Amendment against technologically induced identification features.[87] A debate exists as to whether subjecting a person to facial recognition technology, which may allow law enforcement to use their face to incriminate them, will violate the Fifth Amendment.[88]

---

[81] *See* O'Harrow, *supra* note 13.

[82] There must be a limit to the growth of what one can 'knowingly' expose to the public, but the Supreme Court has yet to define such a limit.

[83] Kasindorf, *supra* note 28.

[84] *Kyllo*, 533 U.S. at 40; *see also supra* notes 73-75 and accompanying text.

[85] *See id.*; Lyman, *supra* note 16.

[86] *See Kyllo*, 533 U.S. at 40; *Dow Chemical*, 476 U.S. at 231.

[87] *See* Gilbert v. Cal., 388 U.S. 263 (1967).

[88] The Fifth Amendment states: "No person shall . . . be compelled in any criminal case to

1. Background Regarding Fifth Amendment Jurisprudence and Biometrics

There is no case law concerning the use of facial recognition technology in the context of the Fifth Amendment, but the Supreme Court has examined other biometric technologies to determine whether their use violates the principles of the Fifth Amendment. In *Gilbert v. California*,[89] the Court held that the use of biometric handwriting exemplars as a means of identifying suspected criminals did not violate the defendant's right against self-incrimination.[90] The Court reasoned that a "mere handwriting exemplar, in contrast to the content of what is written," is a physical characteristic and thus falls outside of the Fifth Amendment's protection.[91] In *United States v. Dionisio*,[92] the Court ruled that voice exemplars used for comparison of recorded conversations in evidence do not violate the Fifth Amendment because compelled displays of identifiable physical features do not infringe upon an interest protected by the Amendment.[93] Justice Stewart, writing for the majority, held that the body is an identifying physical characteristic outside the Fifth Amendment's protection, provided that law enforcement uses the biometric technology to measure a person's physical properties and not as a testimonial or communicative form of evidence.[94]

2. The Constitutionality of Facial Recognition Technology Within the Meaning of the Fifth Amendment

It appears that the use of facial recognition technology as a form of public security is in harmony not only with the Fourth Amendment, but it also does not violate the Fifth Amendment. It does not matter that facial recognition as presently used involves a compelled display of physical features whereby a person is forced to submit their image for the software's use, because the Supreme Court has not found fault in such compelled displays.[95] Law enforcement only uses the software as a means of identifying actual or suspected criminals.[96] It does not serve as a testimonial or communicative form of guilt since a system match only alerts authorities that a subject from

---

be a witness against himself . . . ." U.S. CONST. amend. V.

[89] 388 U.S. 263 (1967).

[90] *Id.* at 266.

[91] *Id.* at 266-67.

[92] 410 U.S. 1 (1973).

[93] *Id.* at 5-6.

[94] *Id.* at 7. The dissenting judges argued only the reasonableness of forcing the suspects to submit to the exemplars in connection with the evidence that had been proffered. *See id.* at 16 n.14.

[95] *Id.* at 5-6 ("It has long been held that the compelled display of identifiable physical characteristics infringes no interest protected by the privilege against self-incrimination.").

[96] *See FaceIt*, *supra* note 11.

the database is located in a given area and has no bearing on that subject's guilt or innocence.[97] Therefore, facial recognition technology would not violate the Fifth Amendment.[98]

One may argue that the cases presented above involve individualized suspicion and thus do not apply to the use of facial recognition technology in public areas. However, this argument falls short. Facial recognition technology, generally, can only be said to impinge upon an individual's Fifth Amendment rights when the system produces a facial match in a crowd, identifying a person already in the database.[99] The fact that the system has already identified and singled out a person by means of having his image included in the software's database due to prior illegal activity or evidence pointing to such, indicates that individualized suspicion is indeed present in the software's use. The individualized suspicion present in the creation of the database reconciles the use of facial recognition technology with the aforementioned cases.

D. Congressional and State Regulation of the Use of Facial Recognition Technology

Although acceptable law enforcement use of facial recognition technology appears to be constitutional, some limits on its use must be put into practice to ensure that the technology is not abused in a way that *would* violate the Constitution. Based on the inadequacy of self-regulation and the vast potential for abuse of constitutional rights by law enforcement, such guidelines must come from a federal regulation outlining the permissible uses of facial recognition technology. In the wake of new technology and advances, however, Congress remains silent, declining to extend its citizens protection from continuous technologically assisted surveillance.[100] Several federal regulations demonstrate this silence.

1. Title III of the Omnibus Crime Control and Safe Streets Act of 1968

After the Supreme Court's decision in *Katz*, Congress reacted by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[101] and in the process set up regulations for the interception of electronic, wire, and oral communications.[102] Title III requires law enforcement to apply for a court order to capture communications in association with the investigation of

---

[97] *Id.; see also supra* note 93 and accompanying text.

[98] *See Dionisio*, 410 U.S. at 7; *Gilbert*, 388 U.S. at 267.

[99] *See FaceIt*, *supra* note 11.

[100] Burrows, *supra* note 54, at 1096 (noting Congressional refusal to protect citizens from video surveillance intrusions).

[101] 18 U.S.C. §§ 2510-2522 (1994).

[102] *Id.*

crimes listed in the provision.[103] Despite Congress' attempt to create a thorough regulation in response to the *Katz* decision, they did not include law enforcement's use of video surveillance in Title III's guidelines.[104]

2. USA-PATRIOT Act

In the USA-PATRIOT Act of 2001,[105] Congress again turned a blind eye to the use of facial recognition technology.[106] The Act primarily focuses on wire, oral, and electronic interception of terrorist information by the FBI and the means of freezing bank accounts and other terrorist assets.[107] It does call for a feasibility study of biometric fingerprint identifiers at offices abroad and at points of entry into the U.S., but it does not address the ability of facial recognition technology to assist in such measures, perhaps due to the lack of prior legislation and judicial guidance.[108]

3. The Aviation Security Act of 2001

Even in the specific context of airport security, Congress has overlooked the regulation of facial recognition technology. The Aviation Security Act of 2001[109] calls for the Transportation Security Administration, among other things, to train airport security personnel, establish a program to use federal marshals as security on flights, and improve airport perimeter access

---

[103] *Id.* at § 2516.

[104] After the Electronic Communications Privacy Act of 1986 added electronic mail, cellular phones and other new technology to the reach of Title III, Congress, in the report accompanying the amendment, addressed the reason why video surveillance was once again left outside of the scope of Title III:

> [I]f law enforcements officials were to install their own cameras and create their own closed circuit television picture of a meeting, the capturing of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. Intercepting the audio portion of the meeting would be an interception of an oral communication, and the statute would apply to that portion.

S. REP. No. 541, at 16-17, *reprinted in* 1986 U.S.C.C.A.N. 3570-3571. It appears that Congress has decided that the regulation of video surveillance is not within the same sphere of electronic communication interception as other Title III surveillance. *Id.*

[105] USA-PATRIOT ACT OF 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[106] As perplexing as it may seem given the current push for more stringent security measures at airports and other areas of national security, the issue of facial recognition technology is found nowhere in the record. *See* 147 CONG. REC. 7207 (2001). The focus of Congress in drafting this bill was primarily on visa and passport issues in relation to national security. *Id.*

[107] USA-PATRIOT Act tit. II-III, 115 Stat. 278-342.

[108] *Id.* § 1008, 115 Stat. 395.

[109] Aviation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

security.[110] Incredibly, the screening of individual passengers is absent, as is a strong push to use facial recognition technology and other biometrics as a security measure.[111] Although Congress has failed to regulate or condone the use of facial recognition technology in this Act, it has at least noted the significance the technology and other forms of biometrics may have in safeguarding our nation's airports in the future by providing funds for the research and development of such technologies.[112]

4. The Federal Intelligence Surveillance Act and The Privacy Act of 1974

While Congress continues to ignore the regulation of technologically-assisted surveillance in both specific law enforcement operations and in general public surveillance, it has, ironically, been willing to address other video surveillance issues. Congress regulated the standards for video surveillance conducted by government agents operating abroad through the Federal Intelligence Surveillance Act.[113] Congress has not promulgated rules regarding the actual collection process of information through surveillance, but oddly it has as regulated the use and dissemination of such information by federal agencies through the Privacy Act of 1974.[114] Federal agents and law enforcement are free from both of these provisions because neither restricts nor lists requirements for video surveillance of U.S. citizens on public streets.[115] The ineffectiveness and inconsistency of current Congressional approaches illustrate that a comprehensive policy or regulation is needed in order to clarify

---

[110] *Id.* §§ 105-106, 111, 115 Stat. 606-610, 616-620.

[111] *Id.* § 106, 115 Stat. 608-610. Section 106 of the Bill does mention the use of biometrics as a means for securing airport perimeter screening. However, in contrast to the other mandatory duties in the section placed upon the Under Secretary of Transportation for Security, § 106(a)(4)(E) provides that the Secretary "may provide for the use of biometric or other technology that positively verifies the identity of each employee and law enforcement officer who enters a secure area of an airport." *Id.* This duty to implement biometrics is permissive, not mandatory, and furthermore, it only provides for the use of biometrics in screening airport personnel and law enforcement. *See id.* § 106(a)(4)(E).

[112] *Id.* § 137, 115 Stat. 637-639 (allowing Congress to appropriate $50,000,000 for the research and development of biometrics and other advanced technologies for the fiscal years of 2002 to 2006).

[113] 50 U.S.C. §§ 1801-1811 (1994). This Act does not apply to surveillance of U.S. citizens by domestic agents. *Id.* Congress passed the Act in 1978 in order to regulate the executive branch's "previously unchecked discretion in conducting electronic surveillance to gather foreign intelligence information." Gregory Birkenstock, Note, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 844 (1992). Essentially, the Act is a compromise, protecting United States citizens against privacy invasions while giving the executive branch leeway to conduct foreign intelligence surveillance. *See id.*

[114] 5 U.S.C. § 552(a) (1974).

[115] Burrows, *supra* note 54, at 1098.

the appropriate uses of facial recognition technology and other high-tech forms of surveillance so that law enforcement can best exploit their capabilities to achieve proper ends.

5. California's SB 169

California's State Legislature is the only state legislature to restrict facial recognition technology use. The legislature drafted Bill SB 169,[116] with the intent of restricting the use of this technology in order to protect both personal privacy and the security of any collected data.[117] The bill ensures that law enforcement does not use biometrics to create a database of information on innocent and unsuspecting citizens.[118] It also requires explicit notice through the use of signs stating that law enforcement is using facial recognition technology, imposes civil fines for the misuse of the technology, and mandates that law enforcement discard biometric identifiers after they fail to match any of the identities stored in a given database.[119] It also restricts the use of facial recognition technology by people, businesses, and other private entities privy to situations in which "it is reasonably necessary to protect public safety or personal property, or to protect against a violation of law."[120]

Bill SB 169, as originally drafted, severely limited the effectiveness of facial recognition technology.[121] The original bill required a warrant prior to any use of facial recognition technology by law enforcement, a measure that seemed to attempt to squeeze this technology into the blanket of regulation found in Title III.[122] Although the aforementioned guidelines concerning signage and the control of biometric databases seem to be logical regulatory measures, § 1798.88, which prohibited almost any use of facial recognition technology by government agents absent a warrant, went too far in protecting against the abuse of this technology.[123] The warrant requirement would, in essence, eliminate the ability of law enforcement to monitor areas vital to national

---

[116] S.B. 169, 2001 Leg., 2001-2002 Session, (Ca. 2001) (amended Sept. 14, 2001). The California Senate defined facial recognition technology as:

> the use of a facial image recorded with a camera or other imaging device used in combination with a system to record and translate facial features, or the spatial relationships between facial features, into mathematical patterns or a unique numerical template, commonly called a faceprint, that can be stored and compared to other data or photos and used to identify a person.

Id. § 2.

[117] S.B. 169, 2001 Leg., 2001-2002 Session (Ca. 2001) (amended Jul. 5 2001).

[118] *Id.* at § 1.

[119] *Id.*

[120] *Id.* § 1798.89(a) (explaining in detail the ways in which the private sector can use facial recognition technology, specifically barring certain practices.).

[121] *Id.*

[122] *Id.*; 18 U.S.C. §§ 2510-2522.

[123] S.B. 169, § 1798.88.

security.[124] The system could not monitor a crowd for criminals because it would filter the images of those not authorized in the warrant.[125] Thus, law enforcement could only use facial recognition technology to monitor specific individuals present in a given area, negating any value it may have in protecting the public at large.

Although the bill's safeguards represented good faith measures to control the abuse of facial recognition technology, the warrant requirement rendered them useless. The California Senate recognized this and struck § 1798.88 from SB 169.[126] The amended SB 169, void of the warrant requirement, reflects the overall notion that a provision enumerating safeguards and restrictions on the use of this technology is more valuable than a provision with a warrant requirement.

IV. THE EMPTINESS OF GOVERNMENTAL THREATS AND THE LACK OF INCENTIVES RENDERS INDUSTRY SELF-REGULATION INEFFECTIVE

Before addressing the ways in which the Identix framework can feasibly be implemented, this Note must address the issue of industry self-regulation to illustrate why there is a great need for Congress to pass a regulation specifically addressing facial recognition technology.

In the past, skeptics, wary of the influence that profits have on American corporations, have denounced attempts by industry to control the use of its own products.[127] The logic is that Congress should not leave manufacturers of facial recognition technology to regulate themselves merely because courts have refused to regulate the use of the technology.[128]

The United States, in exercise of its privacy policy, has generally asked for self-regulation in industries where the potential for abuse exists.[129] In industries such as facial recognition technology, where the potential for abuse

---

[124] *See Letter Regarding CA Legislation*, *supra* note 2.

[125] *See FaceIt*, *supra* note 11.

[126] S.B. 169, 2001 Leg., 2001-2002 Session (Ca. 2001) (amended Sept. 14, 2001).

[127] Amato, *supra* note 6 (quoting Barry Steinhardt of the ACLU, "We can't leave this to systems designers or the marketplace."); Roger Clarke, *Biometrics and Privacy*, AUSTRALIANNATIONALUNIVERSITY.EDU, *at* http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html (Jan. 21. 2002) (stating that effective self-regulation is a "highly unlikely result in a world that demands corporations act to maximize profit, market-share, and shareholder value").

[128] James Glover, *New Try at Privacy Regulation*, WIRED.COM, *available at* http://www.wired.com/news/topstories/0,1287,13158,00.html (Jan 17, 2002) (quoting Jason Catlett, Chief Executive of Junkbusters, an online consumer advocacy group, "By self-regulating, [industries] can keep the enforcement mechanisms non-existent, or under their own control, so they don't have the inconvenience of legal sanctions").

[129] Froomkin, *supra* note 25, at 1525 (noting the government's approval of online merchants' use of TRUSTe.com in order to verify the existence of privacy policies).

is relatively high, the U.S. fails to provide legal sanctions as an incentive to enforce self-regulation.[130] Instead, the incentive comes from the mere threat of governmental regulation.[131] Without the threat of government regulation, the economic incentive to provide strong privacy protections to the subjects of the technology is faint, nonexistent, or unevenly distributed throughout the marketplace.[132] The reliance on threatened regulation seems to be a futile measure designed as a political strategy to avoid the arduous process of regulation.[133] The threat of regulation appears to be a way for legislators to "pass the buck" to the industry in the hopes that a threat will force the industry to react, reducing the chance that legislators must regulate in an area of uncertainty.[134]

In the case of the facial recognition technology industry, reliance on the regulation threat alone may have no impact nor provide any incentive to self-regulate.[135] Some facial recognition software manufacturers have been quite open with their belief that until government regulations are put into place, they are under no obligation to provide guidelines and security procedures to ensure protection of privacy rights.[136] Designers feel that it is not their job to be "gatekeepers looking out for how the technology ultimately is used."[137] Current attempts by the facial recognition technology industry to self-regulate include information on potential abuse of the technology, but without any guidance about how to combat the abuse.[138] The industry has met these self-regulatory attempts with little enthusiasm and much contempt.[139]

---

[130] *Id.* at 1527.

[131] *Id.* at 1524.

[132] *Id.*; Clarke, *supra* note 126 ("Market forces are subject to many imperfections, and it is in the economic self-interest of individuals and corporations to exploit these imperfections and to generate new ones."); *see also* Roger Clarke, *The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies*, *at* http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html (Jan. 17, 2002) ("Wolves self-regulate for the good of themselves and the pack, not the deer.").

[133] Froomkin, *supra* note 25, at 1527 ("It is hard to believe that the strategy is anything more than a political device to avoid regulation.").

[134] *Id.* at 1527-28.

[135] Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 789 (1999) (noting that only when U.S. industry perceived government threats of regulation as being credible did U.S. industry take the issue of privacy more seriously).

[136] Amato, *supra* note 6 (quoting DARPA manager Jonathan Phillips: "We develop the technology. The policy and how you implement them is not my province").

[137] *Id.* (quoting Robert Collins, a facial recognition software developer at Carnegie Mellon).

[138] International Biometric Industry Association, *International Biometric Industry Association Privacy Principles*, *at* http://www.ibia.org/privacy.htm (Sept. 17, 2001). The IBIA's Privacy Principles simply inform the reader that there is a potential for the abuse of

This evidence, illustrating disregard for the threat of regulation, suggests that comprehensive regulation is necessary in order to effectively regulate and manage the use of facial recognition technology.[140]

V. IMPLEMENTING VISIONICS' FRAMEWORK INTO A COMPREHENSIVE REGULATION OF FACIAL RECOGNITION TECHNOLOGY

While Congress has continually ignored placing restrictions on the use of facial recognition technology, the Identix Corporation has addressed the potential for abuse. Identix has called for regulations that will regulate where and for what reasons the software should be employed, and establish safeguards to protect the privacy rights of citizens who are affected by the software's use.[141]

The Identix Corporation correctly states that the nation's best defense against future terrorist attacks rests in the ability to prevent terrorists and other individuals who pose a danger from boarding planes or gaining access to secure areas.[142] It also correctly attempted to regulate the use of facial recognition in a way that maximizes national security without compromising the public's civil liberties.[143] Such regulation of facial recognition technology ensures that the public respects the technology for its capabilities rather than fears the technology for its potential for abuse.

While *Protecting Civilization* outlines only a system for the use of facial recognition technology in airports, the framework can be made applicable to other areas of national security such as nuclear power plants, borders and points of entry, national monuments, and important government buildings such as the Capitol and the White House. The final portion of this Note analyzes the Identix framework, providing commentary and suggesting ways that Congress can implement the framework to regulate the use of facial recognition technology in all areas of national security.

A. Security through Intelligence-Based Identification

Identix's position is that, in the current crisis, people do not have an absolute right to fly; rather it is a privilege for those who do not pose a terrorist

---

facial recognition technology and that appropriate measures must be taken, without providing any guidance. *See id.*

[139] Clarke, *supra* note 126 (describing the IBIA's Privacy Principles as "a trivial document whose sole function is to convey concern, and which contributes nothing whatsoever to the protection of the people forced to submit to biometric measurement").

[140] *Id.* (arguing that it is necessary to look at solutions other than self-regulation for protection).

[141] Protecting Civilization, *supra* note 9.

[142] *Id.* at 1 (noting that any defense that our country may implement to secure our airports must be "within the context of a free and open society").

[143] *Id.*; Burrows, *supra* note 54, at 1083.

threat.[144] Identix identifies facial recognition biometrics as the most effective available means to identify those who pose a threat to national security.[145]

Although Identix does not call for limits on the technology's use, the framework identifies five essential areas in which regulation can improve airport security and rebuild public confidence without creating unnecessary burdens on travelers.[146] These areas include (1) facial screening at border control/general crowd surveillance at high risk areas such as airports; (2) biometric-based boarding processes that would prevent terrorists from boarding planes; (3) a more thorough means of screening airport employees than the guidelines provided by the Aviation Security Bill; (4) stricter physical access to secure areas; and (5) intelligence data mining to develop and maintain terrorist watch lists.[147]

The framework's five areas represent applications that would best take advantage of facial recognition technology. The framework is adaptable and law enforcement can implement it in other areas of national security. The framework also ensures that law enforcement can secure entry points, restrict access to sensitive areas, constantly update and maintain databases to avoid the perilous consequences of obsolete information. Finally the framework ensures that employees do not pose security risks. Therefore, the Identix framework for airport security may also provide a suitable framework for other areas of national security.

By limiting the use of the technology to areas where we are most vulnerable, Identix has created a way in which facial recognition technology can enhance security without deeply threatening personal privacy.[148] The framework does not call for blanket use throughout the country on public streets, but rather it calls for the use of facial recognition technology in a controlled atmosphere by qualified law enforcement agents.[149] Congress can adopt this approach by limiting the areas in which law enforcement can use facial recognition technology as a surveillance/security measure. Such an approach would effectively ensure use primarily as a security measure designed to identify potential terrorists.

---

[144] Protecting Civilization, *supra* note 9, at 1.

[145] *Id*. at 2. (finding that "Biometrics have been under development for more than a decade. Nevertheless, wide scale adoption has in the past been hampered by technical immaturity, hardware costs, as well as legitimate concerns over privacy. Today, the technology has reached sufficient levels of maturity and stability and, by adhering to industry standards for responsible use, can be deployed without posing a threat to our privacy.").

[146] *Id*. at 1-5.

[147] *Id*.

[148] *Id.* at 2.

[149] *Id.* at 1.

B. Implications for Privacy

More important than where and in what manner law enforcement will use facial recognition technology, is what safeguards should Congress formulate to ensure responsible and ethical use of the technology.

Identix believes that the cornerstone of responsible use lies in public notice guidelines, database integrity, a no match-no memory system requirement, procedures for operation and access, and enforcement and penalty guidelines.[150] An analysis of each of these areas reveals that Congress can effectively safeguard the privacy rights of those affected by facial recognition technology through rigid regulation.

1. Public Notice Guidelines

Public notice guidelines are necessary to communicate the goals and capabilities of facial recognition technology to the public. A Congressional mandate requiring signage in areas where the technology is used does not seem like an overly burdensome measure, nor would it create a significant financial burden. In fact, such mandates are in place in cities that presently employ facial recognition technology in public areas.[151] California's Bill SB 169 lays out the requirements for signage and public knowledge and Congress could use this as a model for this privacy safeguard.[152]

Congress should, however, also give law enforcement some wiggle room by creating exceptions to the notice requirement. Congress should excuse situations in which the notice requirement would severely hamper the ability of law enforcement to maintain appropriate levels of security. Such situations may include authorized undercover investigations, intelligence gathering initiatives, high alert levels of security, and other instances where the security situations may compromise the integrity of law enforcement. Thus, the notice requirement would not pose the threat of being counter-productive to law enforcement's capacity to identify and detain dangerous individuals.

2. Database Integrity

Perhaps the most important aspect of privacy safeguards involves the creation of the database and the problem of identifying exactly whose images the system should include. Congress must be careful here because under-inclusion may cause public outrage if the system is unable to detect a threat to public safety. Conversely, over-inclusion would subject more people to potential invasions of privacy than necessary, again triggering public outrage.[153]

---

[150] *Id.* at 7.

[151] Kasindorf, *supra* note 28.

[152] SB 169, § 1798.87, 2001 Leg., 2001, 2001-2002 Session (Ca. 2001).

[153] The invasion of privacy contemplated by this suggestion involves having one's image

Currently, watch list databases primarily include felons, sexual predators, wanted criminals, and missing children.[154] While some individuals from these groups may pose risks to the public safety, few pose the type of risk associated with terrorist attacks and national security. In order to use facial recognition technology to create a national shield against terrorist attacks, databases must include suspected or known terrorists, and others individuals determined to pose a national security risk.[155] Such a database would be most effective if created on a nationwide level, and would eliminate the need for each state or district to create and maintain its own database. Congress must establish guidelines that require justification for the inclusion of an individual in a watch list database.[156] Such guidelines may be based on reliable and accurate reports by law enforcement officials, both foreign and national, that include known offenses committed by an individual, suspected activities, and the potential threat the person poses to the public.

The now defunct warrant requirement of SB 169 could prove very useful in this area.[157] Instead of requiring a warrant for the use of facial recognition technology, Congress should require that law enforcement could only include an individual in the database pursuant to a warrant. Law enforcement could turn over the information collected by the database to a federal judge who would make the final decision as to whether law enforcement was justified in including a person in a database. Such a measure would place an appropriate check on law enforcement's ability to create databases and further serves privacy protection. It is also apparent that such a proposal would place an enormous burden on any judge, but given the ongoing national security crisis, this burden is justified. The events of September 11th have altered everyday life with airport security frisking citizens and asking people to take their shoes off, while armed guards now greet people on their way into work.[158] Increasing the nation's security is not an easy and burden-free task. The same strains and pressures placed on the American public should be placed on the legal system and our elected officials so that the transition to this new way of life can be as smooth and effective as possible.

Congress must also require that law enforcement update database

---

as part of a law enforcement database. Such an inclusion, as noted in the discussion of the Fifth Amendment's role in facial recognition technology, would be akin to individualized suspicion. Thus, an erroneous inclusion could have an impact on the privacy of an innocent person.

[154] *Face Recognition*, *supra* note 35; Kasindorf, *supra* note 28.

[155] *Protecting Civilization*, *supra* note 9, at 2.

[156] *Id.* at 7.

[157] S.B. 169 § 1798.87.

[158] Jeffrey Rosen, *A Cautionary Tale for a New Age of Surveillance*, N.Y. TIMES ON THE WEB, *available at* http://devney.net/greypapers/a_cautionary_tale_for_a_new_age_of_surveillance.htm (Oct. 7, 2001).

information to make certain that the system does not become over-inclusive. Any regulation should provide sunset provisions for removing individuals previously detained by law enforcement, but who no longer pose a threat after the mandatory updates. In order to lessen the strain this process poses on federal judges, the sunset provision should also require a court to review an individual for removal from the database. These reviews should take place annually, as opposed to more frequent reviews. Under such a review, law enforcement officials would have to petition a federal judge for the continued inclusion of an individual in the database, with the judge having the final judgment on whether a person still poses enough danger to the public to warrant continued inclusion in the database. As a facial recognition database poses a potential for abuse, the swift and accurate removal of individuals from a database by law enforcement and judicial officials will restrict the number of individuals in a database and ensure that only those who truly pose a threat to the public are included.

Congress has the means to regulate the review, disclosure, and sharing of information contained in databases by incorporating provisions of both the Privacy Act of 1972 and the Patriot Act of 2001. The Privacy Act establishes strict guidelines that secure any information in or passing through the database system.[159] The Patriot Act would allow for the creation of a complete database by permitting extensive sharing of intelligence between U.S. agencies as well as between the U.S. and other countries.[160] By pooling intelligence resources from around the globe through this Act, law enforcement could establish a more complete database of suspected or known terrorists.[161]

3. No Match-No Memory

Congress should take measures to compel manufacturers to design facial recognition technology software that instantly purges a scanned image failing to create a match within the system. This is necessary to restrict the use of the technology so that law enforcement can use it for security purposes alone, as there are no compelling reasons why facial recognition software should not instantly erase images that do not generate a match.[162] California uses this rule and Congress should follow.[163]

This regulation would not create a financial burden because this capability

---

[159] PRIVACY ACT OF 1974, 5 U.S.C. § 552(a) (1974).

[160] USA-PATRIOT ACT OF 2001, Pub. L. No. 107-56, §§ 1801-1811, 115 Stat. 272 (2001).

[161] *Id.*

[162] Burrows, *supra* note 54, at 1113.

[163] S.B. 169, § 1798.88.

already exists.[164] The financial burden will only come through including the technology in the systems, a cost that will inevitably be passed to the consumer. If Congress does not require this limitation along with location restrictions for facial recognition technology use, law enforcement with access to a system could arguably keep track of a person's whereabouts on a consistent basis, an Orwellian notion that raises a plethora of privacy concerns.[165]

Either Congress can regulate the specifications of facial recognition technology to safeguard against abuse of this type or it can impose self-regulation. Although, Part IV of this Note denounced self-regulation as an ineffective measure, severe government-imposed sanctions and fines would be an appropriate and successful way to guarantee industry cooperation.[166]

4. Authorized Operation and Access

A regulation requiring authorized operation and access must also include appropriate guidelines. It seems that Congress should give law enforcement and other necessary public officials the responsibility to monitor and control facial recognition technology.[167] There is much public concern that some individuals currently responsible for security at airports and other private industries such as nuclear power plants may be incapable of ensuring public safety.[168] Until the private sector improves security requirements, Congress should limit access to facial recognition technology to appropriate law enforcement and government officials.[169] Congress should delegate the responsibility to manage and install facial recognition technology, at least in the contexts of airports and similar locations, to the Transportation Security Administration, as they do with many other security related issues covered in the Aviation Security Bill.[170]

Once Congress establishes who has the duty of managing and operating the systems, it should establish funding for training programs to guarantee that those in charge of facial recognition systems can accurately monitor and run

---

[164] *FaceIt*, *supra* note 11.

[165] Burrows, *supra* note 54, at 1128 (noting that facial recognition technology and other forms of video surveillance can be perceived as unreasonable intrusion if used to "track a person from block to block without her knowledge to focus on a letter she is reading, words she may be mouthing or an itch she may be scratching").

[166] Reidenberg, *supra* note 134, at 789.

[167] Bray, *supra* note 41.

[168] Raphael Lewis, *Logan Will Test Face-Data Security*, BOSTON GLOBE, Oct. 25, 2001, at B1 (noting that airports and other industries in the private sector generally contract their security out to the lowest bidding companies, who in turn hire inexperienced and unqualified people).

[169] Bray, *supra* note 41.

[170] Aviation Security Bill of 2001, Pub. L. No. 107-71, § 137, 115 Stat. 597 (2001).

them. Congress could generate this funding through the appropriation of a study and development of biometrics under the Aviation Security Bill.[171] After responsible officials have received the proper training, a complex system of logons, encryption and security is needed to properly protect against unauthorized access and unauthorized use of the system.

A regulation governing facial recognition technology should require the use of backup systems to prevent inaccurate and false systems matches.[172] Congress would also be prudent in delegating the establishment of the procedures for response to matches to an agency such as the F.B.I. or the C.I.A. If Congress does not create such protocols, it will leave decisions regarding the nature of investigation and detainment to those most ill equipped to handle such responsibility, such as low-level employees as is the case under the current system of security.[173]

Detainment and investigation procedures need to be on a scaled basis with greater police powers given to law enforcement when individuals known to be terrorists or determined to pose a substantial risk to public safety are detected. This measure will again enforce the principle that facial recognition technology seeks to deter terrorism and protect the public, not subject individuals to unwarranted burdens to their civil liberties.[174]

5. Enforcement & Penalty

Congress must enforce its imposed guidelines for the regulation to have any weight. The Federal Aviation Administration, currently in charge of airport security, is a logical choice for the monitoring and enforcement of facial recognition technology in airports. Similarly, the Nuclear Regulatory Commission ("NRC")[175] and Immigration & Naturalization Service ("INS")[176] should be responsible at nuclear power plants and points of entry, respectively. Random inspections of facilities and oversight procedures will ensure that law enforcement will follow guidelines.

---

[171] *Id.*

[172] Froomkin, *supra* note 25, at 1178.

[173] Lewis, *supra* note 167.

[174] *Protecting Civilization*, *supra* note 9, at 2.

[175] The NRC's "primary mission is to protect the public health and safety, and the environment from the effects of radiation from nuclear reactors, materials, and waste facilities"; regulating "these nuclear materials and facilities to promote the common defense and security." *See What We Do, at* NRC.gov, http://www.nrc.gov/what-we-do.html (Mar. 25, 2002).

[176] The INS "is a Federal agency within the US Department of Justice (DOJ) that administers the nation's immigration laws." *See* Immigration and Naturalization Service Web site, *Missions, Strategies, and Performance*, http://www.ins.usdoj.gov/graphics/aboutins/insmission/index.htm (Last modified Dec. 13, 2002).

Congress should include civil penalties for violations and criminal penalties for truly egregious violations. It should specifically subject manufacturers not conforming to congressional mandates as to the specifications of their products to fines. Monetary fines and disciplinary measures would help to reduce the possibility of unauthorized use of facial recognition technology by law enforcement officials. Congress may provide for increased penalties for more serious violations of privacy principles, such as suspect database integrity.[177]

In the case of a false system alert resulting in illegal detainment or interrogation, Congress should place the onus on the facial recognition technology industry, indemnifying law enforcement officials acting in accordance with the law. Such a burden would provide an incentive for manufacturers to produce accurate software and to continually improve upon the level of sophistication and capability of this technology. An indemnification clause would also allow law enforcement, acting in accordance with the law, to effectively monitor and control security, without the threat of lawsuits or disciplinary measures.

VI. CONCLUSION

As the nation recovers from September 11th, the public cry for stronger security measures grows and our political leaders must answer the call and provide for the use of technology that will not only protect our nation from terrorist acts, but will also protect our nation from abuses of constitutional rights.

Facial recognition technology may not be the perfect solution to protect high-risk security areas, but it is currently a viable option that when properly used is constitutional and effective, as law enforcement can use the technology in a manner that comports with the Fourth and Fifth Amendment.[178] The plain view doctrine and the accessibility to the public, bring facial recognition technology within the boundaries of the Fourth Amendment.[179] Similarly, the Supreme Court's refusal to categorize the use of certain biometric devices as a testimonial or communicative form of guilt, and facial recognition technology's similarity to these devices will allow law enforcement to monitor public areas without violating the Fifth Amendment.[180]

While regulating the use of and calling for the research and development of various forms of sense-enhancing technology, Congress has continually overlooked the ability of facial recognition technology as an effective public shield.[181] Lack of congressional regulation and the inability of self-regulation

---

[177] *Protecting Civilization*, *supra* note 9, at 7.

[178] Scheeres, *supra* note 18; Burrows, *supra* note 54, at 1083.

[179] Kyllo v. U.S., 533 U.S. 27 (2001); Dow Chemical Co. v. U.S., 476 U.S. 227 (1986); Katz v. U.S., 389 U.S. 347 (1967).

[180] U.S. v. Dionisio, 410 U.S. 1 (1973); Gilbert v. U.S., 388 U.S. 263 (1967).

[181] Froomkin, *supra* note 25, at 1527.

to protect citizens from the misuse of the technology leads to the conclusion that Congress must promulgate a comprehensive directive to ensure that law enforcement's use of facial recognition technology stays within the boundaries of the Constitution.

Recognizing that private industry is ill-equipped to design specific measures and regulations, the Identix approach is exactly what it claims to be: a framework.[182] It is a skeletal approach that addresses many of the important issues concerning facial recognition technology, but it is rudimentary and would require revision and "fill" to have practical application.

While some may still question the motives behind the framework, Identix has excelled at identifying and highlighting the many areas of security that facial recognition technology could enhance, while also identifying privacy risks associated with the technology and ways that these risks can be eliminated.[183] It is a framework that can be completed so that Congress can create a comprehensive regulation of the use of facial recognition technology.

At this time, it is important that the call for increased security measures and protection from terrorism does not trample the rights the Constitution gives to us. Such protection can only be found in a comprehensive guideline that will best utilize the benefits of facial recognition technology while guaranteeing that it is not misused. It is the onus of Congress to decide whether they wish to accept the enormous task of finishing what Identix has started.

---

[182] *Protecting Civilization*, *supra* note 9, at 1 (Identix did not attempt to propose legislation or policy for its customers, it merely suggested practical ways that facial recognition technology could be used and provided an incomplete framework to be filled in by those with the expertise and knowledge to do so).

[183] *See id.* at 2.