1-1-2006

Catching up to Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology

Rudy Ng

Follow this and additional works at: https://repository.uchastings.edu/hastings_comm_ent_law_journal

Part of the Communications Law Commons, Entertainment, Arts, and Sports Law Commons, and the Intellectual Property Law Commons

Recommended Citation
Available at: https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol28/iss3/3

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Communications and Entertainment Law Journal by an authorized editor of UC Hastings Scholarship Repository. For more information, please contact wangangela@uchastings.edu.
Catching Up To Our Biometric Future: Fourth Amendment Privacy Rights and Biometric Identification Technology

by Rudy Ng*

I. Introduction ........................................................................................................... 425
II. Overview of Biometric Recognition Technology .............................................. 428
   A. Biometrics ........................................................................................................ 428
   B. Fingerprints ................................................................................................... 429
   C. DNA .................................................................................................................. 430
   D. Iris Scanning .................................................................................................... 431
   E. Facial Recognition Technology ....................................................................... 432
III. Fourth Amendment Privacy Rights ................................................................... 433
   A. Biometrics ........................................................................................................ 433
   B. Compulsory DNA Sampling of Convicted Felons ......................................... 435
   C. DNA Data Bank Expansion .......................................................................... 436
IV. Legislative Considerations .................................................................................. 439
   A. The Future for Emerging Biometrics ............................................................... 439
V. Conclusion ............................................................................................................. 442

I. Introduction

The concept of identifying people via their unique biometric identifiers is not a new idea. It has long been recognized that a person’s fingerprint is a unique way to identify that person.¹ However, some more recent advances in technology have called into question the constitutionality of these new forms of biometric

---

¹ University of California, Hastings College of the Law, J.D. Candidate, 2006; San Francisco State University, M.S. in Biochemistry, 2001; University of California, Berkeley, B.A. in Biochemistry, 1996. I would like to thank my family and friends for their loving support and encouragement, especially Queenie Mak for editing this Note and for keeping me sane throughout this adventure called law school.

identification. After the September 11, 2001, terrorist attacks, one of our primary concerns has been ensuring for our homeland security. New, more rigorous forms of biometric screening have been proposed and implemented in some instances. For example, San Francisco International Airport has installed hand geometry identification stations for employees in some secure areas. Before being allowed to proceed into restricted areas, employees must place their hand on a biometric reader, which scans their hand and compares it to images stored in a database.

Another area of concern is tracking known or suspected criminals. A proposed method to achieve this is to use face recognition technology which can quickly scan an individual's facial geometry from a surveillance video and attempt to match that person's face to a database of millions of known or suspected criminals. The science fiction movie Minority Report illustrated the use of iris scanners not only to provide positive identification of individuals who had been apprehended by the police, but also to identify ordinary citizens walking down the street in order to project personalized advertisements to them. The future may not be as far away as we think. Foreign and domestic banks have experimented with the use of fingerprint and iris scanning technologies in ATMs. In addition, police in London, England have been using face recognition technology as part of their Citywatch program aimed at reducing crime in the community. The question is how far we are willing to take this technology, especially in regards to tracking known or suspected criminals.

6. Id.
Catching up to Our Biometric Future

In *United States v. Kincade*, the Ninth Circuit upheld the constitutionality of the DNA Analysis Backlog Elimination Act of 2000, which required certain convicted felons to submit blood samples from which authorities could obtain their DNA profile. Convicted felons' DNA profiles are kept in a DNA data bank to either provide evidence against or exonerate them if they were ever suspected of another crime. This ruling by the Ninth Circuit could potentially pave the way to requiring convicted felons to submit to the collection of other types of biometric identification data, such as iris or face recognition scans. As with current DNA databases, iris and face recognition data would then be stored in databases and shared with authorities throughout the nation. Tracking suspected criminals could be as easy as matching an image of their face from a surveillance video at their local shopping mall to an image in the face recognition database. How far are we willing to invade the privacy rights of individuals in the name of security?

These concerns are not restricted to convicted felons. While there are statutes in all fifty states which require certain convicted felons to submit DNA samples so law enforcement can maintain their DNA profile, these DNA data banks are being supplemented with DNA profiles from people who have been arrested but have not been convicted of crimes. If people not convicted of any crimes are being included in DNA data banks, then is this opening the door for the collection of other types of biometric data, such as face or iris recognition data, from people who are merely suspected of committing a crime? Is this the beginning of the slippery slope that may lead us to a world where a person suspected of committing a crime has to seek out an unscrupulous back-alley physician to perform an eye transplant surgery in order to maintain his or her freedom and privacy, as in the movie *Minority Report*? Clearly there are other concerns besides keeping our streets safer by making it easier for law enforcement personnel to identify recidivist activities.

---

12. Id. at 840 (holding that "compulsory DNA profiling pursuant to the federal DNA Act would have occasioned no violation of Kincade's Fourth Amendment rights.").
13. Id. at 819-20.
17. CA Prop. 69 (approved by voters Nov. 2, 2004).
Part II of this note is an overview of biometric recognition technology, especially iris scanning and face recognition technology. Part III provides an analysis of individual privacy rights under the Fourth Amendment in relation to biometric technology, the compulsory DNA sampling of convicted felons, and DNA databases, especially in light of recent Federal Court of Appeals decisions and recently passed legislation. Part IV presents legislative considerations for the collection of less invasive biometric data that is easier to collect and monitor passively, such as facial recognition data. Finally, Part V provides a summary of the discussion.

II. Overview of Biometric Recognition Technology

A. Biometrics

Biometrics refers to the automated methods of identifying a person based on their unique physical characteristics. In a typical application, an individual’s physical traits are scanned by a machine and then a comparison is made to a database containing previously stored information about that individual. This process is used to positively identify the individual and is referred to as verification, or one-to-one matching. For example, one-to-one matching could be used at a security checkpoint before allowing individuals access to restricted areas of a building. Biometric scanning can also be used to identify a person by comparing their biometric data to all of the records that have been stored in the database. This process is referred to as identification, or one-to-many matching. For example, one-to-many matching could be used to identify an unknown person by trying to match their biometric data to the data of known individuals saved in a database.

22. Woodward, supra note 2, at 100. See also Feldman, supra note 19, at 656.
23. Woodward, supra note 2, at 100. See also Feldman, supra note 19, at 656.
24. Woodward, supra note 2, at 100. See also Feldman, supra note 19, at 656.
B. Fingerprints

Historically, fingerprints have been the most common and widely accepted form of biometric identification. Fingerprint identification has been used by law enforcement since the early twentieth century. Fingerprint identification initially required the fingerprint examiner to go through the tedious process of manually comparing ink fingerprints fixed onto fingerprint cards. This process was very time consuming and could often take months to complete. However, the fingerprint identification process has been computerized and automated. The Federal Bureau of Investigation (FBI) now uses the Integrated Automated Fingerprint Identification System (IAFIS). IAFIS contains the fingerprints and corresponding criminal history information for more than 47 million subjects, making it the largest biometric database in the world. The process of matching fingerprints, which used to take months to complete, can now be performed in a few hours. For example, the FBI can identify an unknown person who left a latent fingerprint at a crime scene by comparing the crime scene fingerprint to the IAFIS database.

Fingerprint identification involves comparing an individual's unique ridge formations or patterns found on the fingertips. These fingertip patterns include ridge formations called whorls, arches and loops. Fingerprint identification relies on the empirically validated assumptions that no two persons have the exact same arrangement of ridge patterns on their fingertips, and that an individual's fingerprints remain unchanged throughout their life.

26. Woodward, supra note 2, at 104.
28. Id.
29. Id.
30. Id.
31. See supra note 27.
32. Id.
33. Id.
34. See supra note 1.
35. See supra note 9, at 431.
36. See supra note 1.
An advantage of fingerprint identification is that it is widely accepted by the public and law enforcement as an accurate and repeatable means for identifying individuals. In addition, finger scanning technology is a quick, non-invasive method of gathering biometric data. A disadvantage of finger imaging is that dirt, oils or cuts on a person’s finger can lead to errors in the results.

C. DNA

Another, more modern, biometric identification technique involves the use of deoxyribonucleic acid (DNA). Each cell in a person’s body contains DNA. DNA is composed of nucleotides arranged in a three-dimensional double helix, and comprises an individual’s heritable genetic material. DNA has useful forensic applications because the sequence of nucleotides of every individual is unique (except for identical twins), which makes DNA ideal for identification purposes.

Two commonly used techniques for DNA identification are Restriction-Fragment-Length-Polymorphism (RFLP) analysis and the Polymerase Chain Reaction (PCR). RFLP analysis is based on naturally occurring minor differences in each person’s DNA sequence. Since each individual’s DNA sequence is unique, by selectively visualizing the areas where these minor differences occur, forensic examiners can determine an individual’s “DNA fingerprint.” PCR is a method of making many copies of a specific segment of DNA. PCR is useful for testing very small samples. For example, the DNA from a tiny amount of tissue or blood found at

---

37. Woodward, supra note 2, at 105.
38. Moo-Young, supra note 9, at 432.
39. Id. at 433.
42. Id. at 8.
43. Id. at 409.
44. Id. at 402-03.
45. Id.
46. Campbell, supra note 41, at 409.
47. Id. at 399, 401.
48. Id.
a crime scene can be amplified into a useable amount via the PCR method.\(^49\)

Similar to fingerprinting, an advantage of DNA analysis is that it is widely accepted by scientists, the public and law enforcement as an accurate and repeatable means for identifying individuals.\(^50\) For example, the FBI has implemented the Combined DNA Index System (CODIS), which allows crime laboratories across the nation to electronically compare the DNA profiles of subjects.\(^51\) However, a disadvantage of DNA identification is that it involves more physically invasive techniques, such as taking a blood sample or buccal swab.\(^52\) In addition, the RFLP and PCR methods must be performed under laboratory conditions, so test results are not available immediately.\(^53\)

D. Iris Scanning

Iris scanning utilizes the colored part of the eye surrounding the pupil, known as the iris, as the biometric characteristic for identification.\(^54\) The iris contains a multitude of structures\(^55\) that uniquely identify an individual.\(^56\) A high-resolution video camera captures an image of the iris, which is then automatically compared to images stored in a database.\(^57\) Iris scanning technology is utilized around the world at airports, prisons, hospitals, and schools\(^58\) and has potential uses in the banking industry at ATMs.\(^59\)

An advantage of iris scanning is that the entire process typically takes about two or three seconds, making results immediately available.\(^60\) In addition, an accurate image of an iris can be taken from up to three feet away, so iris scanning is a non-invasive
A disadvantage of iris scanning is that, while it may be relatively unobtrusive, current iris scanning technology still requires the cooperation of the subject in order for the camera to take a useable image of the iris (i.e. the user must look straight into the camera without blinking). However, future advances in iris scanning technology may allow systems to surreptitiously take iris scans at greater distances. Also, although iris scanners are able to take an image of an iris through clear eyeglasses or contact lenses, iris scanners are ineffective if the user is wearing sunglasses or eyeglasses with a reflective coating.

E. Facial Recognition Technology

The final method of biometric identification discussed here is facial recognition technology. Facial recognition technology involves taking a picture of a subject’s face or capturing their image from video surveillance. The system then processes the image and converts it into a digital template based on the geometry of the individual’s face. Finally, the individual's biometric data is matched against data stored in a database.

An advantage of face recognition technology is that it is a very unobtrusive biometric identification technique. Surveillance cameras can capture images of an individual’s face without the individual’s knowledge or cooperation. In addition, face recognition technology can match individuals despite changes in their expression, facial hair, or hair style. The main disadvantage of face recognition

61. Id.
64. McGuire, supra note 62, at 448.
65. Moo-Young, supra note 9, at 437.
66. See Birmingham City Centre CCTV Installs Visonics; FaceIt, supra note 10, at 3; supra note 7.
67. Moo-Young, supra note 9, at 437.
70. Moo-Young, supra note 9, at 437. See also Indentix, http://www.identix.com/trends/face.html (last visited Mar. 8, 2006).
technology is that it has a lower accuracy rate than other biometric identification techniques.\textsuperscript{72} In addition, if the subject's face is not properly illuminated due to poor lighting conditions, shadows, or glare, then the accuracy of face recognition technology is reduced further.\textsuperscript{73}

\section*{III. Fourth Amendment Privacy Rights}

\subsection*{A. Biometrics}

The Fourth Amendment to the United States Constitution protects individuals from being subject to "unreasonable searches and seizures."\textsuperscript{74} The United States Supreme Court addressed privacy under the Fourth Amendment in \textit{Katz v. United States}.\textsuperscript{75} The Court, while noting that the "Fourth Amendment cannot be translated into a general constitutional 'right to privacy,'" held that the Fourth Amendment does "protect individual privacy from certain kinds of governmental intrusion."\textsuperscript{76} \textit{Katz} provided a two-pronged test for determining when a governmental action constitutes an unreasonable search.\textsuperscript{77} The two factors a court should consider are whether an individual has an actual subjective expectation of privacy and whether that expectation is one that society is willing to objectively recognize as reasonable.\textsuperscript{78} Subsequently, the Court has held that no reasonable expectation of privacy exists for things that an individual exposes to the eyes of the public.\textsuperscript{79}

More recently, in \textit{Kyllo v. United States},\textsuperscript{80} the Court faced the issue of whether the Government's use of a thermal imaging device to scan a private home constitutes a search under the Fourth Amendment.\textsuperscript{81} In \textit{Kyllo}, agents from the Department of the Interior across the street from petitioner's home used a thermal imager to determine whether heat was emanating from petitioner's home

\begin{thebibliography}{99}
\bibitem{note72} Feldman, \textit{supra} note 19, at 658-59.
\bibitem{note73} See \textit{supra} note 71.
\bibitem{note74} U.S. CONST. amend. IV.
\bibitem{note75} \textit{Katz} v. United States, 389 U.S. 347 (1967).
\bibitem{note76} \textit{Id.} at 350.
\bibitem{note77} \textit{Id.} at 361.
\bibitem{note78} \textit{Id.}
\bibitem{note79} California v. Ciraolo, 476 U.S. 207, 215 (1986) (applying the \textit{Katz} two-prong test to a situation where police flew over respondent's house in an airplane and observed marijuana plants growing in respondent's backyard).
\bibitem{note80} \textit{Kyllo} v. United States, 533 U.S. 27 (2001).
\bibitem{note81} \textit{Id.} at 29.
\end{thebibliography}
consistent with the use of special lights to grow marijuana. Although the Government argued that the petitioner had no subjective or objectively reasonable expectation of privacy because the heat was being radiated from the external surface of the house, the Court held that the agents' activity did constitute a search and was presumptively unreasonable without a warrant. However, the Court limited its holding to apply to situations where the "Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion." This preserves the notion that the Fourth Amendment does not protect an individual's privacy when he willingly exposes something to the public.

In order for biometric identification methods to pass muster under the Fourth Amendment, they must be reasonable. In determining whether a search is reasonable, a court must balance the extent of the intrusion on an individual's Fourth Amendment rights against the government's legitimate interests in effectuating the search. In addition, reasonableness depends on the circumstances in which biometric identification is used. The government may have compelling interests in certain areas, such as providing for secure air travel, which argues in favor of the promotion of biometric identification systems in airports. However, it is less clear how significant an interest the government may have in other areas, such as achieving secure ATM transactions or identifying convicted felons from a crowd of people. These concerns are only magnified in light of the advances in biometric technology which make it easier to surreptitiously collect biometric data, such as face recognition images.

Although the use of biometrics such as iris scanning and face recognition technology has not been addressed by the Court, the

82. Id. at 29-30.
83. Id. at 35, 40.
84. Kyllo, 533 U.S. at 40.
86. Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 652 (1995) ("As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness'").
87. Id. at 652-53 (citing Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 619 (1989)).
analytical framework established by Katz can be applied to the use of emerging biometric technology.\textsuperscript{89} Keeping in line with its previous holdings, the Court would most likely hold that an individual should have no expectation of privacy while in a public place.\textsuperscript{90} Individuals who are out in public places have chosen to expose themselves to the public, whether it be to other people or to surveillance cameras enabled with face recognition technology.\textsuperscript{91} In addition, it is likely that modern society's increased desire to protect public safety would outweigh individuals' privacy interests when they are in public.\textsuperscript{92} Thus, future face recognition and iris scanning technologies fall short of constituting an unreasonable search under the Court's current Fourth Amendment jurisprudence.\textsuperscript{93} Therefore, the government should be free to use these types of biometric technology in public places without violating an individual's constitutional privacy rights.\textsuperscript{94}

B. Compulsory DNA Sampling of Convicted Felons

All fifty states and the District of Columbia have statutes that require mandatory collection of DNA samples from individuals convicted of certain crimes.\textsuperscript{95} In 1998, the California Legislature enacted Chapter 696, which created the DNA and Forensic Identification Data Bank.\textsuperscript{96} Under California Penal Code § 296, anyone convicted of certain sex offenses, murder, voluntary manslaughter, felony spousal abuse, aggravated sexual assault of a child, certain felony offenses of assault and battery, kidnapping, mayhem, or torture was required to submit a blood and saliva sample from which the individual's DNA could be obtained.\textsuperscript{97} In 2002, California Penal Code § 296 was amended by Chapter 906, which expanded California's compulsory DNA sample submission legislation to include individuals convicted of committing or

\textsuperscript{89} Mallon, \textit{supra} note 85, at 977-78.
\textsuperscript{90} \textit{Id.} at 976-77.
\textsuperscript{91} \textit{Id.}
\textsuperscript{92} \textit{Id.} at 977-78.
\textsuperscript{93} \textit{Id.}
\textsuperscript{94} Mallon, \textit{supra} note 85, at 978.
\textsuperscript{97} \textit{Id.} at 220-21.
attempting to commit other felonies, including first-degree burglary, first-degree robbery, specific types of arson, and carjacking.\(^{98}\)

The recent case, *United States v. Kincade*,\(^{99}\) examined the Fourth Amendment constitutionality of a federal statute similar to California Penal Code § 296. Under the DNA Analysis Backlog Elimination Act of 2000,\(^{100}\) individuals who have been convicted of certain federal crimes must provide federal authorities with a biological sample of their DNA.\(^{101}\) The Ninth Circuit held that convicted felons have substantially diminished expectations of privacy because, once convicted, the individual’s identity becomes a matter of state interest.\(^{102}\) In addition, there are overwhelming societal interests supporting the collection of DNA information from convicted felons, such as providing a deterrent effect helpful in reducing recidivism.\(^{103}\) Accordingly the Ninth Circuit held that compulsory DNA profiling of convicted felons does not violate an individual’s Fourth Amendment rights.\(^{104}\)

While the Ninth Circuit’s ruling in *Kincade* reinforces the constitutionality of the collection of DNA information from convicted felons, it is still unclear how courts would rule on the collection of other types of biometric data, such as iris scans or facial images. In formulating its holding in *Kincade*, the Ninth Circuit emphasized the point that extracting a blood sample from an individual amounted to only a minor intrusion into an individual’s personal privacy and bodily integrity.\(^{105}\) This indicates that courts may look more favorably on biometric identification techniques that pose an even lower threat of intrusion into an individual’s bodily integrity, such as iris scanning or facial imaging.

C. DNA Data Bank Expansion

Bolstered by the Ninth Circuit’s ruling in *Kincade*, the California Legislature proposed Proposition 69 on the November 2004 ballot.\(^{106}\)

---

98. Id. at 222.
101. Kincade, 379 F.3d at 816-17.
102. Id. at 837.
103. Id. at 838-39.
104. Id. at 840.
Proposition 69 sought to amend California Penal Code § 296 to require DNA profiling of all of California's convicted felons, not just those convicted of serious felonies as in the previous statute. In addition, beginning in 2009, Proposition 69 would require adults arrested or charged with any felony offense to submit a DNA sample, regardless of whether they were subsequently convicted of the offense or not. The legislative findings accompanying Proposition 69 indicated that the state had a compelling interest in expanding its DNA data bank to provide for the "accurate identification of criminal offenders" and to "ensure that persons wrongly suspected or accused of crimes are quickly exonerated so that they may reestablish their standing in the community." The voters approved Proposition 69 on November 2, 2004.

In upholding existing statutes requiring convicted felons to submit samples to DNA data banks over Fourth Amendment challenges in *Kincade*, the Ninth Circuit emphasized the fact that convicted felons have minimal expectations of privacy. However, in contrast to convicted felons, individuals who have merely been arrested or charged, but not convicted of any felony, do not have a reduced expectation of privacy in providing their genetic information. Furthermore, the government interest in deterring recidivist activity is lessened when non-convicted individuals are involved. Thus, the government's interest in improving the identification techniques used by law enforcement may be outweighed by the non-convicted individual's interest in keeping their genetic information private.

Proposition 69 does contain a provision whereby an individual who has submitted their DNA sample for inclusion into the DNA data bank can have their DNA specimen destroyed and their database file expunged. However, in order to qualify for this provision, the individual must not be charged or convicted of the

---

110. *See Greg Lucas and Vanessa Hua, State Propositions; Proposal to Expand DNA Database on Criminals Headed for Approval, S.F. CHRONICLE, Nov. 3, 2004, at B3.*
111. *See Kincade, 379 F.3d at 840.*
112. *Id.* at 837.
113. *Taylor, supra* note 95, at 537.
114. *Id.* at 538.
115. *Id.* at 537.
underlying offense that served as the basis for their inclusion into the DNA data bank.\textsuperscript{117} To have their DNA specimen destroyed and their record expunged from the DNA data bank, the individual must file a written request with the state's DNA Database and Data Bank Identification Program.\textsuperscript{118} Despite the inclusion of this provision into Proposition 69, a non-convicted individual's privacy rights may be more fully protected if their DNA specimen was destroyed and database file was expunged automatically, rather than only upon a written request.

Iris scanning and facial imaging provide a less intrusive method for collecting biometric data than DNA sampling. With regard to convicted felons, the government would have the same compelling interests present with the collection of biometric data as it does with requiring DNA samples.\textsuperscript{119} Thus, the application of traditional Fourth Amendment principles to emerging biometric identification technologies, such as iris scanning and facial recognition technology, suggests that courts would uphold the use of biometrics in conjunction with convicted felons.\textsuperscript{120} In addition, courts would also likely uphold statutes requiring the inclusion of these types of biometric data into data banks of convicted felons.\textsuperscript{121} However, with regard to non-convicted individuals, the government's interest in collecting other forms of biometric identification data becomes less compelling, especially if non-convicted individuals' biometric data is being included in biometric data banks.\textsuperscript{122} Because of the ease and speed that automated biometric identification systems can perform one-to-one or one-to-many matching, inclusion of non-convicted individual's biometric data into biometric data banks justifiably fuels people's fears of having the Orwellian Big Brother monitoring their every move.\textsuperscript{123} Clearly, important legislative considerations must be addressed as we rapidly catch up to the future of biometric identification technology.

\begin{footnotes}
\footnote{117. \textit{Id.}}
\footnote{118. \textit{Id.}}
\footnote{119. \textit{See} Cal. Legis. Serv. Prop. 69 (2004).}
\footnote{120. \textit{See generally} Taylor, \textit{supra} note 95, at 537-38. \textit{See also} Cameron, \textit{supra} note 96, at 226-28.}
\footnote{121. \textit{See} Taylor, \textit{supra} note 95, at 537-38. \textit{See also} Cameron, \textit{supra} note 96, at 226-28.}
\footnote{122. \textit{See} Taylor, \textit{supra} note 95, at 537-38. \textit{See also} Cameron, \textit{supra} note 96, at 226-28.}
\footnote{123. Mallon, \textit{supra} note 85, at 955.}
\end{footnotes}
IV. Legislative Considerations

A. The Future for Emerging Biometrics

The Court has not spoken on the issue of the Fourth Amendment constitutionality of emerging biometric identification technology, such as iris scanning and face recognition technology. However, the current legislative and legal framework that has been applied to existing biometric identification techniques, such as DNA profiling, can be extended and revised to accommodate these emerging technologies. In formulating this framework, it is important to keep in mind the tension between the principle that an individual has no privacy rights while in public and the ideal that an individual may have enhanced privacy rights against the surreptitious collection of biometric data. Striking the proper balance and reaching an acceptable compromise between these two principles should be one of the goals of future legislation in the area of biometric identification technology.

Facial recognition technology is intimately tied to the use of cameras or video surveillance equipment. One of the first large scale uses of face recognition technology occurred at the 2001 Super Bowl in Tampa, Florida. Police employed video surveillance cameras set up at the stadium entrances and face recognition technology to scan 100,000 faces at stadium turnstiles and compare them to a database of 1,700 criminals. This led the ACLU to dub the event the “Snooper Bowl.” The system identified nineteen matches, however, police determined that eighteen of those were false matches. When police were dispatched to find the one positive match, the suspect had disappeared by the time officers arrived on the scene. This illustrates a drawback to face recognition technology in that video surveillance is an inherently passive activity. Although face recognition technology may be able to pick out suspects from large crowds, it does not prevent crime or even ensure that police officers will be able to apprehend the suspect.


125. Id.

126. Id.

127. Id.

128. Id.
Interestingly, the Vermont Supreme Court has upheld the use of video surveillance when “used in a narrow set of circumstances, where the police had already determined that a crime was being committed, and only as a substitute for in-person surveillance.” However, the court indicated that there may be a Fourth Amendment violation “where video surveillance is aimed indiscriminately at public places and captures lawful activities of many citizens in the hope that it will deter crime or capture what crime might occur.” Thus, even if individuals knowingly expose themselves to public places, the government may run afoul of the Fourth Amendment if it indiscriminately captures facial images of every passerby for comparison to a database of known or suspected criminals, which is exactly what occurred at the 2001 Super Bowl. Therefore, some limitations should be placed on when the government will be allowed to use video surveillance in conjunction with face recognition technology.

For example, law enforcement could be required to have an individualized suspicion or probable cause before allowing them to use face recognition technology in public places. This standard could mirror the requirements law enforcement officers must meet to acquire advance judicial approval of a search warrant. A drawback of such a requirement is that it may hinder the effective deployment of face recognition technology, especially if law enforcement would like to make expeditious use of the technology.

Alternatively, before being allowed to use face recognition technology, law enforcement could be required to meet a standard similar to that required for investigative stops under Terry v. Ohio. In Terry, the Court addressed what standard law enforcement officers must meet in justifying their decision to search people whom they have detained. The Court held that subjective good faith on the part of police officers is not enough. Instead, the Court held that the Fourth Amendment requires police officers to meet an objective reasonableness standard to justify a search in light of the particular

130. Id.
131. Terry v. Ohio, 392 U.S. 1, 21 (1968) (holding that “in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.”).
132. Id. at 21-22.
133. Id. at 22.
circumstances. Applying the Terry standard to face recognition technology, law enforcement agents would have to be able to delineate objectively reasonable facts that, under the circumstances, led them to believe that the use of face recognition technology was necessary to identify the suspect.

In addition, time limitations should be placed on the extent of the usage of face recognition technology. Thus, law enforcement would not be able to set up a camera on a street corner and just wait weeks or months until a suspected criminal happened to walk by and the camera captured his or her image. Moreover, if law enforcement wants to use face recognition technology in conjunction with video surveillance equipment, then cameras should be clearly visible to the public and marked with signs, rather than secretly hidden from the public's view.

Because of the unobtrusive nature of face recognition technology, and perhaps future iterations of iris scanning technology, greater oversight is needed than with DNA database management due to the increased potential for abuse. This is especially true when such technology is employed by the government because the government has the resources to collect and store more information than private parties and the government can also do more damage with the information they collect. DNA data banks were originally created to help solve crimes that involved DNA evidence, not as a means of preventing or deterring future crimes. Following the Ninth Circuit's decision in Kincade, Proposition 69 expanded the scope of California's DNA data bank to include individuals convicted of any felony. Thus, under the Ninth Circuit's approach, it would seem likely that inclusion of a convicted felon's iris scan or facial image into a database would not violate the Fourth Amendment. However, legislation in this area should prohibit law enforcement agencies from supplementing their facial image database with facial scans of innocent private citizens whose facial images happen to be captured by the cameras.

134. Id. at 21-22.
136. Id. at 1431.
137. Herlica, supra note 14, at 953.
138. See Kincade, 379 F.3d at 840.
In addition to expanding the scope of California's DNA data bank, Proposition 69 contains a provision whereby non-convicted or acquitted individuals can request to have their DNA sample destroyed and their DNA data bank file expunged. Similarly, the face recognition and iris scan database records of individuals arrested or charged, but later eliminated as suspects, should be expunged. However, because these types of biometric data may have been obtained surreptitiously, the database records should be deleted automatically, rather than by written request since the individual may not even know of his or her inclusion into the biometric database.

V. Conclusion

As biometric identification technology companies strive to make their products more accurate, faster, and more affordable for the mass market, the public is only likely to see an increase in the use of biometrics in the future. What may have seemed like a fanciful idea in a science fiction movie a couple of years ago may be reality in the near future. As we catch up to our biometric future, the legislature and courts will need to address important Fourth Amendment constitutional questions.

While emerging biometric identification technology, such as iris scanning and face recognition technology, may be a fast, cutting-edge way for law enforcement to keep track of convicted felons and suspected terrorists, the government should not be allowed to unreasonably intrude on individual privacy rights under the Fourth Amendment. Ultimately, the legislature and courts will need to weigh society's need to feel secure against their desire to protect individual privacy and reach a reasonable compromise.

140. Id.
141. Dunn, supra note 57, at C.