South Carolina Law Review

Volume 63
Issue 4 *ANNUAL SURVEY OF SOUTH CAROLINA LAW*
Article 7

Summer 2012

Eyephones: A Fourth Amendment Inquiry into Mobile Iris Scanning

Christopher R. Jones

"EYEPHONES": A FOURTH AMENDMENT INQUIRY INTO MOBILE IRIS SCANNING

I. INTRODUCTION

A. *Setting the Stage*

Imagine for a moment that an American police officer is on duty, patrolling a neighborhood as he has done many times before. As he rounds a corner, he takes notice of someone casually walking down the street, not engaging in any illegal or suspicious behavior. Although seemingly innocuous, however, the

pedestrian does match the description of a suspect in a recent armed robbery that took place nearby. The officer, believing he may have spotted this suspect, pulls over and stops the pedestrian. After speaking with him for a few minutes, the officer reaches for his belt and retrieves a smartphone. He asks the pedestrian if he would consent to having his picture taken, in a sense. The pedestrian, either knowing he has nothing to hide or not wanting to arouse suspicion, agrees, and the officer captures the image—except the image he has captured is not an ordinary photograph. It is a high-resolution image of the pedestrian's eye. The smartphone, in a matter of seconds, analyzes and processes the image, compares the pedestrian's identity to an online database of previously captured images, and returns the results to the officer.

Now, depending upon your point of view—and perhaps also on the result of the hypothetical encounter (whether the pedestrian is in fact the robbery suspect the officer is seeking)—this interaction between the police officer and the pedestrian involves either a fantastic new tool for law enforcement, which will help to keep our streets safer from criminals by denying them the ability to present false identification and escape capture, or an unnerving Orwellian device that facilitates intrusion into one's constitutionally protected right to privacy, only an incremental step removed from the "big brother" state imagined in fiction.[1] However, the interaction described above is not a chapter from George Orwell's *1984* or a scene from *Minority Report*.[2] And, despite any discomfort or misgivings one may have about the hypothetical scenario,[3] the device the officer used to confirm or refute the pedestrian's involvement in the recent robbery is currently on the market,[4] and is being increasingly utilized by police departments across the country, along with a number of other users.[5] Personal beliefs aside, however, the legal legitimacy of this technology ultimately depends on whether the officer's conduct infringed on the pedestrian's Fourth Amendment rights against illegal search and seizure.

When the House of Representatives adopted the Fourth Amendment among the Bill of Rights in 1789,[6] it surely did not envision the scenario described above, at least not in that form exactly. The Fourth Amendment was developed and adopted primarily to prevent the use of general warrants and writs of assistance, which were prevalent in pre-revolutionary America, and which the

---

1. GEORGE ORWELL, 1984 (1949).

2. MINORITY REPORT (Twentieth Century Fox et al. 2002). This film was adapted from an earlier short story. *See* Philip K. Dick, *The Minority Report*, *in* FANTASTIC UNIVERSE, Jan. 1956, at 4 (Leo Margulies ed., King-Size Publications, Inc.).

3. *See, e.g.*, Tovia Smith, *New Police Scanner Raises 'Facial Profiling' Concerns*, NPR (Aug. 11, 2011), http://www.npr.org/2011/08/11/138769662/new-police-scanner-raises-facial-profiling-concerns.

4. *Products & Services*, BI²TECHNOLOGIES, http://www.bi2technologies.com/products (last visited Mar. 26, 2012).

5. *See infra* Part II.B.

6. H.R. JOURNAL, 1st Cong., 1st Sess. 85–86 (1789), *available at* http://memory.loc.gov/cgi-bin/query/r?ammem/hlaw:@field(DOCID+@lit(hj001139)).

founders wanted to ensure did not emerge in the newly formed country.[7] While the founders may not have imagined the technology used in modern society when they drafted the Fourth Amendment, the language they ultimately adopted is broad enough to cover its use. Although some have described the Fourth Amendment as a "mass of contradictions and obscurities,"[8] its broad language has allowed the protections it provides to adapt as necessary to the world in which it operates—to expand and contract as seen fit by the United States Supreme Court,[9] and to bring within its reach new technologies and societal norms as they develop over time.[10]

B. Roadmap

This Note began by establishing a hypothetical scenario upon which the subsequent analysis will be based. The next Part provides basic background information regarding iris scanning in general and MORIS (the new technology described above) in particular. A brief exploration of the influence of contemporary social mores on the Supreme Court's Fourth Amendment jurisprudence follows the background information in an attempt to discover whether current cultural views of technology and its effect on privacy influence the Court's treatment of mobile iris scanners. Part III of this Note consists of a Fourth Amendment analysis of the constitutionality of MORIS based upon the Supreme Court's prior Fourth Amendment jurisprudence. Following the federal analysis, this Part inquires whether the constitution of the State of South Carolina offers any additional protection for the pedestrian in our hypothetical. Finally, this Note concludes by discussing concerns raised by the use of mobile iris scanners and offers suggestions to ameliorate—or eliminate—these concerns.

II. BACKGROUND

A. Iris Scanning Generally

In order to undertake an analysis of the constitutionality of mobile iris scanning, it is important to first understand the science and fundamentals of how iris scanning and recognition works. This begins with a brief lesson in biology.

---

7. *See* Olmstead v. United States, 277 U.S. 438, 463 (1928); Weeks v. United States, 232 U.S. 383, 390 (1914); Boyd v. United States, 116 U.S. 616, 624–27 (1886). *See generally* THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 15–20 (2009).

8. Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468 (1985); *see also* MCINNIS, *supra* note 7, at 5 ("[C]ourts have struggled to come up with a clear understanding of what constitutes a violation of the amendment.").

9. MCINNIS, *supra* note 7, at 43.

10. *See, e.g.*, Kyllo v. United States, 533 U.S. 27 (2001) (analyzing the use of a thermal scanner under the Fourth Amendment).

The iris is a muscle located in the front of the eye, surrounding the pupil.[11] The function of the iris is to change the size of the pupil in order to regulate the amount of light that enters the eye. Formed before birth, one's iris is believed to be unique from all others.[12]

Iris scans are performed by capturing a high-resolution image of the eye using near-infrared (NIR) light.[13] NIR light is used to illuminate the iris without causing discomfort to the subject.[14] Once the image is captured it must be processed in a few different ways. First, the iris is isolated from the rest of the image using landmark features.[15] Isolation is performed so that only the iris, and not the eyelashes or eyelid, is processed for identification.[16] Once isolation is complete, complex mathematical algorithms are performed that encode the visual image of the iris into a digital array, similar to DNA sequencing gel or a complex barcode.[17] It is this "map" of the iris that is then compared to other "maps" saved in a database, either to seek out a match or to compare against a particular entry to confirm or refute an individual's purported identity.[18]

It must be noted at the outset that iris scanning is entirely different from retinal scanning.[19] While iris scanning captures an image of the external, front portion of the eye, retinal scanning captures an image of the retina, which is located at the back, inside the eye.[20] Retinal scanning also incorporates NIR light to illuminate the eye, but uses the unique pattern of blood vessels located on the retina, instead of the color patterns of the iris, to identify a subject.[21]

B. Current Uses

Iris scanning, while still a relatively new form of identification when compared to other methods such as fingerprinting,[22] is beginning to gain traction

---

11. SUBCOMM. ON BIOMETRICS, NAT'L SCI. & TECH. COUNCIL, IRIS RECOGNITION 1, fig.1 (2006), *available at* http://www.biometrics.gov/Documents/IrisRec.pdf [hereinafter NSTC REPORT].

12. *Id.*

13. *See* John Daugman, *How Iris Recognition Works*, 14 IEEE TRANSACTIONS ON CIRCUITS & SYS. FOR VIDEO TECH. 21, 21–22 (2004), *available at* http://www.cl.cam.ac.uk/~jgd1000/csvt.pdf.

14. NSTC REPORT, *supra* note 11, at 2; *see* Daugman, *supra* note 13, at 22.

15. NSTC REPORT, *supra* note 11, at 2.

16. *See id.*

17. *See id.* at 3; Daugman, *supra* note 13, at 22–23.

18. *See* NSTC REPORT, *supra* note 11, at 3 (citing John Daugman, *Mathematical Explanation of Iris Recognition*, UNIV. OF CAMBRIDGE, http://www.cl.cam.ac.uk/users/jgd1000/math.html (last visited Apr. 4, 2012)).

19. *See id.* at 4.

20. *Id.*

21. *Id.*

22. Stephanie Watson, *How Fingerprinting Works*, HOWSTUFFWORKS, http://science.howstuffworks.com/fingerprinting3.htm (last visited Apr. 4, 2012). Fingerprints were used in lieu of signatures in 1858 by Sir William Herschel, Chief Magistrate of the Hooghly district in Jungipoor, India. The first systemic use in the United States was by New York State prisons in 1903. *Id.*

via a number of different uses throughout society.[23] For example, in 2005, the John F. Kennedy Airport in New York implemented a pilot program that utilized iris scanners in order to allow preregistered passengers to circumvent the standard customs procedures and to quickly proceed through the airport.[24] In 2011, the TSA announced plans to implement a nearly identical program to expedite security checks, although the scope of the TSA effort is not yet clear.[25] The New York Police Department already scans the irises of all arrestees to track them through the court system and prevent their escape.[26] Additionally, the Justice Department is partnering with the National Sherriff's Association to implement similar programs in jails across the country in an effort to prevent escapes.[27] In 2010, the Department of Homeland Security began testing the effectiveness of using iris scanners at a border patrol station to track illegal immigrants,[28] and the United States military has used iris scanners in Iraq and Afghanistan to build a database of almost four million residents.[29] Despite its relatively limited use at present,[30] iris scanning technology is gaining acceptance in an increasing number of settings, and is poised to spread considerably over the next few years.

C. MORIS

MORIS, or Mobile Offender Recognition and Identification System, is the technology at the focus of this Note. MORIS is manufactured by BI[2]Technologies.[31] The device is a 12-ounce attachment[32] to the now ubiquitous iPhone,[33] and allows an officer in the field to perform not only an iris scan, as

---

23. The examples in this Part illustrate the current uses of iris scanning technology generally, and do not represent the specific phone-based system that is the focus of this Note.

24. Ian Bishop, *Eye Flight: Iris Scan for JFK Passengers*, N.Y. POST (Jan. 14, 2005, 12:00 AM), http://www.nypost.com/p/news/eye_flight_iris_scan_for_jfk_passengers_SHsHDP5nqtySchjkHsT1aM.

25. *See* Adam Clark Estes, *Coming to an Airport Near You: Iris Scanners*, THE ATL. WIRE (June 7, 2011), http://www.theatlanticwire.com/technology/2011/06/coming-airport-near-you-iris-scanners/38595.

26. Ray Rivera & Al Baker, *New York City Police Photograph Irises of Suspects*, N.Y. TIMES (Nov. 15, 2010), http://www.nytimes.com/2010/11/16/nyregion/16retinas.html.

27. *See* Melanie S. Welte, *Iris Scans May Prevent Mistaken Release of Inmates*, USA TODAY (Feb. 27, 2010, 9:29 AM), http://www.usatoday.com/news/topstories/2010-02-27-2493914959_x.htm.

28. Thomas Frank, *Homeland Security to Test Iris Scanners*, USA TODAY (Sept. 13, 2010, 10:37 AM), http://www.usatoday.com/tech/news/surveillance/2010-09-13-1Airis13_ST_N.htm.

29. *See* Thom Shanker, *To Track Militants, U.S. Has System That Never Forgets a Face*, N.Y. TIMES (July 13, 2011), http://www.nytimes.com/2011/07/14/world/asia/14identity.html.

30. *See* Welte, *supra* note 27.

31. *See Products & Services*, *supra* note 4.

32. Smith, *supra* note 3.

33. *See Apple Reports First Quarter Results*, APPLE (Jan. 24, 2012), http://www.apple.com/pr/library/2012/01/24Apple-Reports-First-Quarter-Results.html (reporting that over thirty-seven million units were sold in the first quarter of fiscal year 2012 alone).

described in the hypothetical, but also facial recognition and fingerprint comparisons,[34] all remotely with no additional equipment required.[35] BI²Technologies' marketing brochure for MORIS claims that the device is "ideal for identifying" sex offenders, illegal immigrants, gang members, individuals with outstanding warrants, parolees, and probationers.[36] It is available only to government agencies and officials,[37] and as of mid-2011, roughly forty law enforcement agencies had ordered approximately one thousand units.[38] Currently, BI² has official endorsements for its line of products from the National Association of Triads (NATI) and the National Sheriff's Association.[39]

III. SOCIETY AS A FOURTH AMENDMENT "BAROMETER"

Justice Oliver Wendell Holmes once referred to the law as a "magic mirror," "wherein . . . we see reflected, not only our own lives, but the lives of all men that have been."[40] Other Justices have repeated the sentiment that the law is an expression of our values as a society, specifically in reference to Fourth Amendment jurisprudence,[41] and it is generally understood that the Court's determination of "reasonableness" as it relates to the Fourth Amendment is shaped in large part by cultural norms.[42] If this premise is true, and the Court does consider societal views in its Fourth Amendment analysis, then it may be

---

34. Smith, *supra* note 3. This Note focuses solely on the device's iris scanning and recognition functions.

35. *See Products & Services*, *supra* note 4.

36. *Mobile, Wireless and Hand Held Offender Recognition and Information System*, BI²TECHNOLOGIES, http://www.bi2technologies.com/sites/default/files/documents/MORIS-Brochure.pdf (last visited Apr. 4, 2012).

37. Brian Heaton, *Iris and Facial Scan Smartphone Nears Mass Release*, GOVERNMENT TECHNOLOGY (July 21, 2011), http://www.govtech.com/public-safety/Iris-Facial-Scan-Smartphone-Nears-Mass-Release.html. As the database against which the iris is compared grows in size, the possibility of false matches will surely grow as well. Whether or not this increase will be significant remains to be seen.

38. *See Smart phone face scan tech a privacy breach?*, CBS NEWS (July 15, 2011, 10:32 AM), http://www.cbsnews.com/stories/2011/07/15/earlyshow/leisure/gamesgadgetsgizmos/main20079772.shtml.

39. *Endorsements*, BI²TECHNOLOGIES, http://www.bi2technologies.com (last visited Apr. 4, 2012).

40. Oliver Wendell Holmes, The Law, Address Before the Suffolk Bar Association Dinner (Feb. 5, 1885), *reprinted in* OCCASIONAL SPEECHES OF JUSTICE OLIVER WENDELL HOLMES, 21 (photo. reprint 1979) (Mark DeWolfe Howe ed., Cambridge, Belknap Press of Harvard Univ. Press, 1962).

41. *See, e.g.*, United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("[I]t is the task of the law to form and project, as well as mirror and reflect.").

42. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (explaining that "dramatic technological change" may change popular attitudes toward privacy expectations); Note, *The Fourth Amendment's Third Way*, 120 HARV. L. REV. 1627, 1628 (2007) ("[I]t is clear that social convention has become the defining ideal of the Fourth Amendment—the source of authority that gives reasonableness its shape."). For the relevance of reasonableness in Fourth Amendment law, see Elkins v. United States, 364 U.S. 206, 222 (1960).

instructive to consider the current relationship our culture has with privacy rights as they relate to technology in general, and to iris scanners in particular.

Our daily lives are becoming increasingly "technocentric"—from our methods of communication with one another[43] to how we encounter the news,[44] and nearly everything in between. We are undoubtedly becoming more dependent on technology to accomplish almost every task. Along with this increasing dependence on technology comes an increase in the sharing of personal information,[45] either with people we know (through social media, perhaps), or with third party entities that assist us in whatever task we are trying to accomplish. As we become more willing to use technology that requires the sharing of information, our expectations of privacy in this information are consequently reduced.[46] It follows, then, given the premise above, that the protection of the Fourth Amendment is similarly reduced in scope.[47]

If the Fourth Amendment protections are constantly being eroded by the ubiquity of technology and information sharing in our daily lives, then one would expect the Supreme Court's Fourth Amendment jurisprudence to reflect this trend. However, two recent cases refute this contention. In *Kyllo v. United States*,[48] the Court determined that the use of a thermal scanner on one's home, without a warrant, constituted a violation of the Fourth Amendment.[49] Additionally, Justice Sotomayor's concurrence in *United States v. Jones*[50] explicitly addressed the increasing dependence upon technology as it relates to invasions of privacy and stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[51] Although these cases seem to counter the premise outlined above, it likely remains true, and yet, while the

---

43. *See, e.g., In U.S., SMS Text Messaging Tops Mobile Phone Calling*, NIELSENWIRE (Sept. 22, 2008), http://blog.nielsen.com/nielsenwire/online_mobile/in-us-text-messaging-tops-mobile-phone-calling (analyzing the increase in the use of SMS text messaging).

44. *See, e.g., Internet Overtakes Newspapers as News Outlet*, PEW RESEARCH CENTER (Dec. 23, 2008), http://pewresearch.org/pubs/1066/internet-overtakes-newspapers-as-news-outlet (reporting that the internet has surpassed all other media except television as an outlet for national and international news).

45. *See Jones*, 132 S. Ct. at 957 (noting that in today's digital age, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 828 (2004) ("New technologies more commonly expose information that in the past would have remained hidden, resulting in meager Fourth Amendment protection in new technologies.").

46. *See* Kyllo v. United States, 533 U.S. 27, 33–34 (2001) (recognizing the "power of technology to shrink the realm of guaranteed privacy"); Kerr, *supra* note 45, at 828; Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 499, 501, 503 (2011).

47. *See* Levy, *supra* note 46, at 504.

48. 533 U.S. 27 (2001).

49. *Id.* at 40.

50. 132 S. Ct. 945 (2012).

51. *Id.* at 957 (Sotomayor, J., concurring).

scope of the Fourth Amendment's protection is slowly narrowing with societal expectations, the Court is reluctant to allow such a change to occur too quickly or without adequate consideration.[52] Consequently, it would seem that, given the limited exposure that iris scanners have attained thus far in society[53] and the natural suspicion that their use arouses in most people,[54] the technology may be circumscribed by our reasonable expectation, or lack thereof, of its adoption by law enforcement for mobile identification.

However, a consideration of the evolution of societal views on privacy and technology, while relevant to a certain extent, may prove not to be determinative in predicting a Supreme Court outcome, and more weight must ultimately be given to the Court's precedent in attempting to accurately predict how the Court will answer the constitutional question that our hypothetical poses.[55]

IV. CURRENT FOURTH AMENDMENT ANALYSIS

A. When Does the Fourth Amendment Apply?

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[56] Therefore, in order for our hypothetical encounter to be within the reach of the amendment, it must first be determined that either a "search" or a "seizure," as defined by the jurisprudence of the Supreme Court, has taken place. However, the inquiry does not end at the mere conclusion that a search or seizure has occurred, for "what the Constitution forbids is not all searches and seizures, but unreasonable searches and

---

52. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

53. *See* Welte, *supra* note 27.

54. *See* Zach Howard, *Police to begin iPhone iris scans amid privacy concerns*, REUTERS (July 20, 2011, 2:59 PM), http://www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720.

55. One could argue that attempting to predict the Supreme Court's decision in a future hypothetical Fourth Amendment case is an effort in futility given the state of its jurisprudence in the area. *See The Fourth Amendment's Third Way*, *supra* note 42, at 1627 (quoting Lloyd L. Weinreb, *Your Place or Mine? Privacy of Presence Under the Fourth Amendment*, 1999 SUP. CT. REV. 253, 253 (1999); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 758 (1994); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 349 (1974)) (noting the obscurity of Fourth Amendment jurisprudence). In addition, attempting to predict the outcome of any Supreme Court case can be described as difficult, at best. *See* Theodore W. Ruger et al., *The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking*, 104 COLUM. L. REV. 1150, 1152 (2004) (stating that legal experts accurately predict Supreme Court case outcomes only 59.1% of the time).

56. U.S. CONST. amend. IV. In *Wolf v. Colorado*, the Supreme Court held that the Fourth Amendment is enforceable against the states, and therefore, against our hypothetical police officer. 338 U.S. 25, 27–28 (1949), *overruled on other grounds by* Mapp v. Ohio, 367 U.S. 643 (1961).

seizures."[57] Therefore, only if it is determined that a search or seizure was unreasonable will the protections of the Constitution take effect.

B. What Is a "Seizure" and When Is It Justified?

What, then, constitutes a seizure for the purposes of our constitutional analysis? It must be noted that there are two types of seizure recognized by the Supreme Court as constitutionally distinct—that of a person and that of property.[58] For purposes of this Note, the concern is only with seizure of a person, and seizure of property will not be discussed.[59] Seizure of a person occurs when a law enforcement officer "restrains [an individual's] freedom to walk away."[60] However, a seizure does not occur merely by the officer approaching the individual and asking questions or engaging him in conversation,[61] even if the officer identifies himself as such[62] or asks the individual for identification.[63] In order for a seizure to occur, there must either be an application of physical force by the officer or a showing of authority to which the individual yields,[64] such that a reasonable person in the individual's position would not believe that he is free to end the interaction.[65]

Having established what constitutes a seizure, one must also consider the circumstances in which a seizure is and is not reasonable for purposes of the Fourth Amendment. The landmark case of *Terry v. Ohio*[66] outlines the Supreme Court's current framework for evaluating the reasonableness of an impromptu stop by a police officer.[67] In *Terry*, the Court stated that there is no black-letter test for determining reasonableness, but that a balancing must be done of the need to search or seize against the invasion to the individual which the search or

---

57. Elkins v. United States, 364 U.S. 206, 222 (1960).

58. *See* Payton v. New York, 445 U.S. 573, 585 (1980).

59. "A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." United States v. Jacobsen, 466 U.S. 109, 113 (1984).

60. Terry v. Ohio, 392 U.S. 1, 16 (1968).

61. *See id.* at 19 n.16; Florida v. Royer, 460 U.S. 491, 497 (1983).

62. *Royer*, 460 U.S. at 497 (citing United States v. Mendenhall, 446 U.S. 544, 555 (1980)).

63. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 185 (2004); *but see* Brown v. Texas, 443 U.S. 47, 50 (1979) (stating that a seizure occurred when police stopped the defendant and asked for identification). The legal distinction between these two cases seems to be that, in *Brown*, the seizure was not a result of the police officers merely asking the defendant for identification. *See Brown*, 443 U.S. at 49. The defendant asserted that the officers had no right to stop him and that the officers frisked him. *Id.* It would seem that the seizure was established by the fact that the officers insisted upon his cooperation and refused to allow him to walk away.

64. *See* California v. Hodari D., 499 U.S. 621, 625 (1991) (citing *Terry*, 392 U.S. at 19 n.16); *Mendenhall*, 446 U.S. at 553.

65. Florida v. Bostick, 501 U.S. 429, 434 (1991) (citing *Hodari D.*, 499 U.S. at 628); *Mendenhall*, 446 U.S. at 554.

66. 392 U.S. 1 (1968).

67. *Id.* at 19–20. Courts often refer to this type of encounter as a "*Terry* stop." *See, e.g.*, *Hiibel*, 542 U.S. at 185.

seizure requires.[68] In determining whether a seizure is reasonable, the "officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[69] The officer's "reasonable suspicion"[70] that the individual is engaging, or has recently engaged in criminal activity, must be founded upon more than a mere hunch,[71] and must be based upon facts that would justify to a reasonable person "that the action taken was appropriate."[72]

Later opinions have supported and clarified the requirements for a justifiable *Terry* stop, stating that courts should take into account the "totality of the circumstances" when determining reasonableness.[73] In addition, the level of suspicion required is less than that needed to establish probable cause.[74] While the threshold level of justifiable suspicion is relatively low, the scope of any detention, once initiated, must be limited to only that which is necessary to effectuate the purpose of the stop.[75]

C. What Is a "Search" and When Is It Justified?

In early decisions regarding the Fourth Amendment, the Supreme Court stated that for a search to occur, there must be either a physical search of a person (i.e., a frisk or pat-down) or a physical invasion into a private area, such as a home or office.[76] However, this line of reasoning was overruled in the landmark case *Katz v. United States*.[77] In *Katz*, the Court declared that FBI

---

68. *Terry*, 392 U.S. at 21 (quoting Camara v. Mun. Court, 387 U.S. 523, 536–37 (1967)); *see also Brown*, 443 U.S. at 50–51 ("Consideration of the constitutionality of such seizures involves a weighing of the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.").

69. *Terry*, 392 U.S. at 21.

70. *Id.* at 37 (Douglas, J., dissenting). This phrase appears only in Justice Douglas's dissent in *Terry*, but has gained widespread acceptance and use in subsequent cases and by the legal community at large. *See, e.g.*, *Hiibel*, 542 U.S. at 185 (using the term "reasonable suspicion" in connection with *Terry*).

71. *See Terry*, 392 U.S. at 22.

72. *Id.* at 21–22. *See also, e.g.*, *Brown*, 443 U.S. at 52 (holding that the contention the suspect "looked suspicious," without any supporting facts, was insufficient to meet the requirements of the Fourth Amendment).

73. *See, e.g.*, United States v. Arvizu, 534 U.S. 266, 277 (2002); Alabama v. White, 496 U.S. 325, 332 (1990); United States v. Cortez, 449 U.S. 411, 417 (1981).

74. *See* United States v. Sokolow, 490 U.S. 1, 7 (1989) (citing *Terry*, 392 U.S. at 30); Adams v. Williams, 407 U.S. 143, 145 (1972) (quoting *Terry*, 392 U.S. at 22).

75. Florida v. Royer, 460 U.S. 491, 500 (1983) ("The scope of the detention must be carefully tailored to its underlying justification."). Moreover, the stop must be limited in duration, while the investigative methods employed need not be the least intrusive means available. *See Sokolow*, 490 U.S. at 11.

76. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 135 (1942), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967).

77. 389 U.S. 347 (1967).

agents violated the defendant's Fourth Amendment rights when they attached an electronic listening and recording device to the outside of a public phone booth in order to eavesdrop on the defendant's phone calls.[78] The Court stated that "the Fourth Amendment protects people, not places,"[79] and that Fourth Amendment protection is not coterminous with a physical intrusion into an enclosure.[80] Expounding on this idea, the Court added a subjective element to the notion of privacy that the Fourth Amendment is willing to protect and stated: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[81] Justice Harlan's oft cited concurrence provided a two-part test that contains both a subjective and an objective element—in order to gain constitutional protection, a person must first "exhibit[] an actual (subjective) expectation of privacy,"[82] and the expectation must be one that society is "prepared to recognize as 'reasonable.'"[83] Twelve years later, in *Smith v. Maryland*,[84] the Supreme Court slightly modified the *Katz* test, stating that there are certain situations in which, due to the subjective expectations of an individual being influenced by notions antithetical to the Fourth Amendment, the subjective prong of Justice Harlan's test can "play no meaningful role."[85] In these situations, the Court stated that "a normative inquiry would be proper."[86] Thus, the subjective element of the *Katz* test was relegated to a lesser significance than the objective element, at least in certain situations. Later, in *United States v. Jacobsen*,[87] the Court stated simply that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[88] This appears to have eliminated the subjective component of the *Katz* test in all circumstances, replacing it with the normative inquiry proposed by *Smith*.

Now that a basic, albeit nebulous, definition of search has been established, when is a search—an invasion of one's reasonable expectation of privacy—constitutionally permissible? Again, our inquiry is limited to our hypothetical scenario, and as such, the probable cause requirement of the Warrant Clause of the Fourth Amendment is not applicable.[89] The Court in *Katz* reiterated the

78. *Id.* at 359.
79. *Id.* at 351.
80. *Id.* at 353.
81. *Id.* at 351 (citations omitted).
82. *Id.* at 361 (Harlan, J., concurring).
83. *Id.*
84. 442 U.S. 735 (1979).
85. *Id.* at 740 n.5.
86. *Id.*
87. 466 U.S. 109 (1984).
88. *Id.* at 113.
89. *See* Terry v. Ohio, 392 U.S. 1, 20 (1968) ("[W]e deal here with an entire rubric of police conduct—necessarily swift action predicated upon the on-the-spot observations of the officer on the

long-standing rule that warrantless searches are per se unreasonable, subject to a limited number of exceptions.[90] Those exceptions include searches incident to a valid arrest, searches justified by exigent circumstances,[91] consent searches, and a number of others not applicable to our hypothetical encounter.[92]

V. THE FOURTH AMENDMENT, APPLIED TO OUR HYPOTHETICAL

A. Is There a Seizure?

As discussed above, whether a seizure occurs depends upon whether there is an application of physical force, or a show of authority, to which the pedestrian yields, and whether a reasonable person in the same situation would believe that he is free to walk away from the police officer.[93] Therefore, whether a seizure occurred in our hypothetical depends a great deal on the behavior of the police officer. If the officer were at any point to physically restrain the pedestrian or state to him that he is not free to leave (and the pedestrian complies), then a seizure did occur.[94]

B. Is the Seizure Reasonable?

The inquiry then turns to whether the seizure is reasonable, and therefore constitutional, under the circumstances. Recall that the reason the officer stopped the pedestrian is because the pedestrian matched the description of the suspect in a robbery that occurred near the hypothetical *Terry* stop. In *Hayes v. Florida*,[95] the Court stated in dicta that the Fourth Amendment would permit a seizure for the purposes of fingerprinting a suspect in the field if there was a reasonable suspicion that the suspect committed a crime, and the officer had a reasonable belief that fingerprinting would establish or negate the suspect's involvement in the crime.[96] The Court qualified this permission, however, stating that the fingerprinting process must be "carried out with dispatch."[97]

---

beat—which historically has not been, and as a practical matter could not be, subjected to the warrant procedure.").

90. *See* Katz v. United States, 389 U.S. 347, 357 (1967).

91. *See Investigations and Police Practices*, 37 GEO. L.J. ANN. REV. CRIM. PROC. 39, 40 (2008). "Exigent circumstances exist when there is probable cause for a search or seizure and the evidence sought is in imminent danger of destruction, the safety of law enforcement officers or the general public is threatened, the police are in 'hot pursuit' of a suspect, or a suspect is likely to flee before the officer can obtain a warrant." *Id.* at 72–74.

92. *Id.* at 40.

93. *See supra* text accompanying notes 64–65.

94. *See supra* text accompanying note 64.

95. 470 U.S. 811 (1985).

96. *Id.* at 817.

97. *Id.*

Therefore, if fingerprinting in the field is permissible, it would seem to follow that mobile iris scanning would also be allowed, subject to the same conditions.

In our hypothetical, the police officer should be able to establish reasonable suspicion that the suspect recently engaged in a crime since the pedestrian matches the description of the robbery suspect. The officer is working off of more than just a hunch, and has particularized facts that should easily justify reasonable suspicion. Following the guidelines laid out in *Hayes*, however, the officer must also have a reasonable belief that scanning the pedestrian's iris would establish or negate his involvement in the robbery, and the iris scan must be carried out expeditiously.[98] The extent to which the iris scan would establish or negate the pedestrian's involvement in the robbery will depend primarily upon the breadth of the database against which the iris scan is compared. It can be reasonably assumed that, since iris scanning is a much newer technology than fingerprinting, the database of irises from past offenders will be smaller than the database of fingerprints that the police department will have on hand. However, it seems logical that police would not use the mobile iris scanners unless they offered an appreciable benefit,[99] and thus it can also be assumed that the likelihood of a suspect being identified in the database is not insignificant.

Additionally, when considering the balancing test outlined in *Terry*,[100] it appears that a mobile iris scan would be more constitutionally permissible than mobile fingerprinting. For example, the need to search or seize is the same regardless of what methods of identification are employed, and the invasion of a suspect's rights is arguably less with a mobile iris scan than with fingerprinting—after all, fingerprinting involves physical contact and perhaps the use of ink that would have to be removed from one's skin, while an iris scan using MORIS requires no more of an invasion than having one's picture taken.

Given the above reasoning, one would be tempted to assume that the constitutionality of mobile iris scanners is a foregone conclusion. However, Justice Brennan's dissent in *Hayes* calls into question the permissibility of on-site fingerprinting.[101] Besides believing that the majority's treatment of the issue was unnecessary,[102] Justice Brennan stated that the constitutionality of on-site fingerprinting would need to be evaluated under the standards laid out by *Terry*, and that, unlike the patdown in *Terry*, the privacy intrusion that on-site fingerprinting entails is not justifiable as necessary to protect the safety of the police officer.[103] The *Hayes* majority, though, did not agree that police safety is

98. *See id.*

99. In fact, law enforcement officers use iris scanners as part of the booking, detention, and release process, so a database of past offenders' iris scans may be nearly as useful as a corresponding fingerprint database. *See supra* text accompanying notes 26–28.

100. *See supra* text accompanying note 68.

101. *See Hayes*, 470 U.S. at 819 (Brennan, J., dissenting).

102. *Id.* at 820. Justice Brennan described the Court's discussion of on-site fingerprinting as "an advisory opinion concerning . . . a police practice that . . . has never been attempted," and stated that the issue was not properly before the Court. *Id.*

103. *Id.* at 819.

the paramount requirement justifying on-site fingerprinting, and stated that reasonable suspicion of complicity in a recent or ongoing crime is all that is needed to satisfy the Fourth Amendment.[104]

In addition to the uncertainty introduced by Justice Brennan's dissent, there is a legally significant difference between fingerprinting and iris scanning that has yet to be explored by the courts—the reasonableness of an expectation of privacy in one's iris as compared to one's fingerprints.[105]

C. Is There a Reasonable Expectation of Privacy in Irises?

Katz states that what a person knowingly exposes to the public is not protected by the Fourth Amendment.[106] Under this reasoning, the Supreme Court has ruled that one's face,[107] voice,[108] and handwriting[109] are all physical characteristics constantly exposed to the public that do not warrant the protection of the Fourth Amendment. However, the Court has also ruled that taking the scrapings from underneath a suspect's fingernails does constitute a search, and is therefore under the purview of the Fourth Amendment.[110] In that case, the Court, quoting *Dionisio* and *Terry*, stated that the search went beyond mere physical characteristics that are constantly exposed to the public and constituted a severe intrusion upon the suspect's personal security.[111] In another case, the Court ruled that an employer's use of a breathalyzer test to detect alcohol in employees also constituted a search.[112] The Court reasoned that the test implicated concerns about bodily integrity, similar to those raised by a blood test, and should be protected by the Fourth Amendment.[113] In *Schmerber v. California*,[114] the Court ruled that taking a blood sample from an alleged drunk driver, while the driver received treatment at a hospital for injuries sustained in an accident, was also a search.[115] The Court drew a distinction between searches "involving intrusions beyond the body's surface," and those of a less invasive nature, declaring that a valid arrest, which ordinarily allows the latter class of searches, does not necessarily justify the former.[116]

---

104. *Id.* at 817 (majority opinion).

105. The Supreme Court has been somewhat ambiguous on whether fingerprinting constitutes a search. *See* Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 8 n.39 (2006) (quoting *Hayes*, 470 U.S. at 814, 817; Cupp v. Murphy, 412 U.S. 291, 295 (1973); Davis v. Mississippi, 394 U.S. 721, 724, 727, 730 (1969)).

106. Katz v. United States, 389 U.S. 347, 351 (1967).

107. United States v. Dionisio, 410 U.S. 1, 14 (1973).

108. *Id.*

109. United States v. Mara, 410 U.S. 19, 21 (1973).

110. *See Cupp*, 412 U.S. at 294.

111. *Id.*

112. Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616–17 (1989).

113. *Id.*

114. 384 U.S. 757 (1966).

115. *Id.* at 758, 767.

116. *See id.* at 769.

Under the reasoning of this jurisprudence, it would appear that arguing for a reasonable expectation of privacy in one's irises may be an uphill battle. The Court consistently considers physical characteristics on the surface of one's body to be less deserving of Fourth Amendment protection than internal characteristics and processes, and since the iris lies on the surface of the body the Court may well consider it to be constantly exposed to the public.

However, unlike one's face or voice, the unique patterns of the iris are not easily ascertainable by the general public. In fact, the MORIS system requires a high-resolution camera, used within roughly six inches of a subject's face, to obtain the necessary image for comparison.[117] In other words, while one's eyes may generally be in view of the public, the data contained in one's irises are, unlike voice or facial characteristics, not necessarily "exposed" to the world. In order to capture and make use of the data in an individual's iris, a law enforcement officer needs the aid of technology.

1. Enhanced Senses

The Supreme Court has had a number of occasions to consider the Fourth Amendment implications of technologies that enhance one's vision used to conduct a search. In *Lee v. United States*,[118] the Court stated that the use of visual magnifiers, including bifocals, field glasses, or telescopes, is not forbidden by the Fourth Amendment.[119] Later, in *Dow Chemical Co. v. United States*,[120] the Court ruled that the use of an aerial mapping camera mounted to the floor of an airplane, to take high-resolution images of a chemical plant, did not violate the Fourth Amendment.[121] The Court stated in *Dow Chemical* that "[t]he mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[122]

However, most recently in *Kyllo v. United States*,[123] the Court declared that the warrantless use of thermal scanners by police to detect heat emanating from the walls of a residential home was a violation of the Fourth Amendment.[124] In both *Kyllo* and *Dow*, the Court made special note of the location that was the subject of the surveillance.[125] In *Dow*, the Court pointed out that the area photographed was not one where privacy expectations are traditionally

---

117. *See* Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. DIGITS BLOG (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/.

118. 343 U.S. 747 (1952).

119. *Id.* at 754.

120. 476 U.S. 227 (1986).

121. *Id.* at 238.

122. *Id.*

123. 533 U.S. 27 (2001).

124. *Id.* at 40.

125. *See id.* at 34; *Dow*, 476 U.S. at 237.

heightened, such as one's home and the surrounding curtilage.[126] Additionally, the chemical plant had taken no precautions to ensure that the area could not be aerially photographed.[127] In *Kyllo*, the Court used language from *Dow* and emphasized the fact that the police were using the thermal scanner to obtain information relating to the interior of a home, which it referred to as the "prototypical . . . area of protected privacy."[128] These cases show that the Court, while generally receptive to sense-enhancing technology in the furtherance of searches, still returns to *Katz*'s reasonable expectation of privacy standard, drawing a clear line of demarcation between what is reasonable in private areas as opposed to public (or as in *Dow*, non-private) places.[129]

In addition to the location aspect, the Court also focuses on the general availability of the technologies used in the search. In *Dow*, the Court noted that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[130] The *Dow* Court found that the camera used, while perhaps prohibitively expensive for the average consumer,[131] was commonly used in mapmaking and did not take advantage of any unique technology that was not available to the general public.[132] Conversely, in *Kyllo*, the Court noted that the thermal imaging technology used by the police was not in general public use.[133] The Court addressed this issue head on, citing precedent supporting the inclusion of general availability as a factor in determining reasonableness of privacy expectations, and it explicitly refused to "reexamine that factor."[134]

The Court's precedent regarding the use of technology to enhance human senses for the purposes of a search suggest that the use of mobile iris scanners, as described in our hypothetical, does not constitute a Fourth Amendment violation. As the Court generally seems to permit the use of sense-enhancing technology so long as the traditional reasonable expectation of privacy is not significantly violated, the fact that an officer's sense of sight is enhanced by MORIS, in and of itself, does not appear to create a constitutional problem. In addition, the iris scans do not require the intrusion into areas of traditionally heightened privacy

126. *Dow*, 476 U.S. at 237 n.4.

127. *See id.*

128. *Kyllo*, 533 U.S. at 34.

129. One commentator noted that the Court's tolerance of sense-enhancing technologies in public places "has left any reasonable expectation of privacy in a public place completely eviscerated." Alexander T. Nguyen, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, 10 (2002).

130. *Dow*, 476 U.S. at 238.

131. The trial court noted that the cost of the camera was in excess of $22,000. *See id.* at 242 n.4 (Powell, J., concurring) (quoting Dow Chem. Co. v. United States, 536 F. Supp. 1355, 1357 n.2 (E.D. Mich. 1982)).

132. *Dow*, 476 U.S. at 238.

133. *Kyllo*, 533 U.S. at 40.

134. *Id.* at 39 n.6.

expectations, as was the case in *Kyllo*. In our hypothetical, the scan is performed on a public street, arguably a location which offers the least expectation of privacy. Furthermore, the technology used to perform the scan is commonly available. MORIS attaches to a standard iPhone and uses the built-in camera to capture the image that is processed for identity comparison.[135] Currently, the iPhone is one of the most used devices around the world for photography,[136] and therefore, the Court is unlikely to determine that the use of MORIS is an unconstitutional invasion of privacy based solely on the technology used.

2. *Abandonment*

However, another distinction can be made between fingerprints and the patterns of irises, which the Court has recognized in other contexts—the fact that fingerprints can be left behind, or "abandoned," on objects touched by an individual, whereas the patterns of one's iris are never abandoned—that is, unless captured by a device such as MORIS. The Court drew this critical distinction as it relates to trash in *California v. Greenwood*,[137] stating that once the defendants placed their trash bags on the curb in front of their home (i.e., a public place), they could not claim a reasonable expectation of privacy in the trash.[138] At least one state supreme court applied this reasoning to DNA left on abandoned objects,[139] and commentators have expressed concerns that the Supreme Court may follow suit.[140] Whether or not this distinction is one that would give rise to a reasonable expectation of privacy in one's irises, however, is unclear, and remains an open question until addressed by the Court.

3. *The Plain View Doctrine*

In addition to the cases presented above, the Court has also developed the "plain view" doctrine as an exception to the general rule that warrantless searches are presumptively unreasonable.[141] The plain view doctrine states that if an object is in plain view—meaning that it can be observed from a legal

---

135. Chloe Albanesius, *Police Depts Deploying iPhone-Based Iris, Face Scanning Tech*, PCMAG.COM (July 14, 2011, 1:10 PM), http://www.pcmag.com/article2/0,2817,2388499,00.asp#fbid=XGMXe8gI0Z5.

136. *See, e.g.*, Nick Bilton, *IPhone 4 Becoming Most Popular 'Camera' on Flickr*, N.Y. TIMES BITS (Apr. 18, 2011, 10:07 AM), http://bits.blogs.nytimes.com/2011/04/18/iphone-4-becoming-most-popular-camera-on-flickr (listing the most used cameras on the popular photo sharing website Flickr).

137. 486 U.S. 35 (1988).

138. *Id.* at 40.

139. *See* State v. Wickline, 440 N.W.2d 249, 252–53 (Neb. 1989) *disapproved of by* State v. Sanders, 455 N.W.2d 108 (Neb. 1990).

140. *See, e.g.*, Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 865 & nn.43–46 (2006) (discussing the many genetic traces that humans unknowingly leave behind).

141. *See* Horton v. California, 496 U.S. 128, 133 (1990).

vantage point—then "neither its observation nor its seizure would involve any invasion of privacy."[142] In our hypothetical, the irises of the pedestrian are in plain view of the police officer. Consequently, the Court could apply this doctrine and hold that viewing (and subsequently capturing in a photograph)[143] the pedestrian's eyes was not a search, and thus, does not violate the Fourth Amendment. Even if the pedestrian were wearing sunglasses, thereby hiding his irises from plain view, courts are in general agreement that the officer could instruct him to remove the glasses without violating the pedestrian's Fourth Amendment rights.[144] However, the plain view doctrine has, thus far, been applied only to the seizure of objects whose incriminating character is immediately apparent,[145] and has not been expanded to include a person's physical characteristics.

VI. SOUTH CAROLINA CONSTITUTIONAL ANALYSIS

Article I, section 10 of the South Carolina Constitution also includes, in addition to the Fourth Amendment's protection against unreasonable searches and seizures, a right against "unreasonable invasions of privacy."[146] This section was amended from its original form in 1967, when the relevant clause was added in order to "take care of the invasion of privacy through modern electronic devices."[147] The South Carolina Supreme Court has subsequently interpreted this clause to offer a higher level of privacy protection than that offered by the Fourth Amendment to the U.S. Constitution.[148] However, to date, the court has

---

142. *Id.* (citing Arizona v. Hicks, 480 U.S. 321, 325 (1987); Illinois v. Andreas, 463 U.S. 765, 771 (1983)).

143. In *United States v. Taketa*, the Ninth Circuit held that videotaping in public places does not violate the Fourth Amendment. 923 F.2d 665, 677 (9th Cir. 1991). The court stated that "the police may record what they normally may view with the naked eye." *Id.* Considering that a video recording is essentially many pictures taken in succession, this reasoning presumptively applies to photographs as well.

144. *See, e.g.*, State v. Shearer, 30 P.3d 995, 1000 (Idaho Ct. App. 2001) ("[T]aking minimal steps to temporarily conceal a facial characteristic that is ordinarily and frequently exposed to the public is, in our view, insufficient to create a legitimate expectation of privacy."); People v. Weekly, 44 Cal. Rptr. 2d 322, 326 (Ct. App. 1995) ("wearing sunglasses [is not] sufficient by itself to establish a reasonable expectation of privacy").

145. *See Horton*, 496 U.S. at 129 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)).

146. S.C. CONST. art. I, § 10 (amended 1967). The full text of this section states: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy 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, the person or thing to be seized, and the information to be obtained." *Id.*

147. COMMITTEE TO MAKE A STUDY OF THE CONSTITUTION OF SOUTH CAROLINA (1895), MINUTES OF COMMITTEE MEETING 6 (Sept. 15, 1967).

148. *See* State v. Houey, 375 S.C. 106, 113, 651 S.E.2d 314, 317 (2007) (citing State v. Forrester, 343 S.C. 637, 645, 541 S.E.2d 837, 841 (2001)); State v. Weaver, 374 S.C. 313, 322, 649

not yet vindicated a defendant's privacy rights solely under the state constitution as related to search and seizure,[149] nor has it offered much in the form of commentary to establish the extent of the higher level of protection that the language offers. Therefore, while the amendment to section 10 seems perfectly suited to establish a heightened expectation of privacy as it relates to systems like MORIS, an assertion that the South Carolina Supreme Court would take the opportunity to acknowledge such a right would only be speculative at this point.

VII. CONCERNS

Having made the case that the use of MORIS would not likely be considered by the Supreme Court to be a violation of the Fourth Amendment, this Part of the Note will address potential concerns that systems such as MORIS raise in a real-world environment.

One major concern regarding the widespread use of an iris scanning system is that it could be used to capture people's iris data without their knowledge or consent. MORIS, according to BI[2] President and CEO Sean Mullin, apparently requires the cooperation of its subject in order to capture a useable image.[150] However, while MORIS currently requires the device to be relatively close to the subject in order to obtain a useable image,[151] even newer cameras allow for an image to be taken up to six feet away,[152] and as technology progresses, so too will the range of the iris scanners.

A related concern that privacy advocates may have with MORIS is the potential of capturing iris information from citizens who ultimately have no criminal record and are of no real interest to police. The makers of MORIS claim that a user's iris information is deleted immediately if no match is found in

---

S.E.2d 479, 483 (2007) (citing S.C. CONST. art. I, § 10 (amended 1967)); *Forrester*, 343 S.C. at 645, 541 S.E.2d at 841.

149. *See, e.g.*, *Houey*, 375 S.C. at 113, 651 S.E.2d at 317 (following analysis under the U.S. Constitution, and finding no violation of rights, the court determined that testing of bodily fluids of offender for disease was "not overly intrusive or so unreasonable as to render the statute violative of the South Carolina Constitution"); *Weaver*, 374 S.C. at 322, 649 S.E.2d at 483 (holding that the provision does not require a warrant before the search and seizure of an automobile located in the backyard of a residence; the focus of the state constitution is "whether the invasion of privacy is reasonable"); *Forrester*, 343 S.C. at 645, 541 S.E.2d at 841 (holding that the state constitution's privacy provision does not require police officers to inform citizens of their right to refuse consensual searches). The court has stated, however, that section 10 does prohibit forced medication solely to facilitate execution of a prisoner. Singleton v. State, 313 S.C. 75, 89, 437 S.E.2d 53, 61 (1993). In addition, it is contended that in *State v. Brown*, 389 S.C. 473, 698 S.E.2d 811 (Ct. App. 2010), the South Carolina Court of Appeals "may have taken the first step in defining an unreasonable invasion of privacy." Jaclyn L. McAndrew, *Who Has More Privacy?:* State v. Brown *and Its Effect on South Carolina Criminal Defendants*, 62 S.C. L. REV. 671, 694–95 (2011).

150. *See* John Cox, *Eyeball-Scanning iPhone Used by Cops to ID Suspects*, CIO (July 21, 2011), http://www.cio.com/article/686547/Eyeball_Scanning_IPhone_Used_By_Cops_to_ID_Suspects; *see also* Howard, *supra* note 54.

151. *See* Steel, *supra* note 117; *see also* Cox, *supra* note 150.

152. Frank, *supra* note 28.

the database;[153] however, without oversight by an independent organization, there is no way to confirm this assertion. Additionally, there are no laws currently in place to ensure that this policy is not changed sometime in the future,[154] resulting in the accumulation of private information to which the police have no valid interest.[155]

Another particularly relevant concern that can be raised concerning iris scanning technology, along with any system of suspect identification, is the accuracy of the technology used, and the potential error rate involved with use of the system. According to John Daugman, who pioneered the iris mapping algorithms embedded in MORIS's software, the theoretical false match rate under real-world conditions is around 1 in 4 million.[156] In addition, BI^{2}Technologies has claimed the system has a "virtual zero error rate,"[157] and that "3.12 billion cross-matches [have been performed] without one false match."[158] In addition to the low theoretical error rate of the matching algorithms, the MORIS system, upon finding a match to a subject's iris, will return a picture of the purported match, allowing the officer to confirm or deny the system's match to an even greater degree of certainty.[159] If the above claims of accuracy are true and translate to actual error rates in the field, then MORIS could prove to provide a relatively low risk of false matches.

Perhaps a more salient concern about the MORIS system lies not in its matching capabilities, but in the method of data transmission that the system employs. As MORIS is an attachment to a consumer smartphone, the system uses existing cellular networks to transmit to, and receive data from, the central database that it searches for a match.[160] As such, the data is vulnerable to interception by hackers and identity thieves.[161] In addition to intercepting the signal to and from the phone, criminals could take advantage of the iPhone's operating system to hack into the phone itself and retrieve data.[162] Another

153. *See Smart phone face scan tech a privacy breach?*, *supra* note 38.

154. *See id.*

155. That type of aggregation of information, known as data mining, is a strikingly common practice among federal agencies. *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2 (noting that fifty-two agencies reported a hundred and thirty-one operational and sixty-eight planned data mining efforts); Kerr, *supra* note 45, at 829.

156. *See* Daugman, *supra* note 13, at 28.

157. RJ Middleton, *iPhone for 'The Man': Face-Recognition Hardware Available*, NBC BAY AREA (Nov. 29, 2010, 9:15 AM), http://www.nbcbayarea.com/news/tech/iPhone-for-The-Man-Face-Recognition-Hardware-Available-110965789.html.

158. *See* Heaton, *supra* note 37 (internal quotation marks omitted).

159. *See Smart phone face scan tech a privacy breach?*, *supra* note 38.

160. *See* Heaton, *supra* note 37 (noting that BI^2, along with the National Sheriff's Association, built and maintain the database used by MORIS).

161. *See* Kate Murphy, *Build Up Your Phone's Defenses Against Hackers*, N.Y. TIMES (Jan. 25, 2012), http://www.nytimes.com/2012/01/26/technology/personaltech/protecting-a-cellphone-against-hackers.html?_r=1.

162. *See* Ben Parr, *iPhone Hack Exposed: The Key Facts*, MASHABLE (July 30, 2009), http://mashable.com/2009/07/30/iphone-hack/.

potential vulnerability is the fact that the database to which the MORIS system connects is accessible on the internet,[163] which leaves it open to attack from traditional hackers who target computer systems as opposed to cell phones.[164]

The final major concern with MORIS, as with any system or procedure adopted by police, is the potential for abuse through selective use, or profiling. Although this concern exists apart from MORIS in particular,[165] the potential invasion of privacy facilitated by this system calls for a heightened awareness of, and active prevention against, such abuse.

VIII. SUGGESTIONS FOR ADDRESSING CONCERNS

In considering the most appropriate approach to take to effectively alleviate the concerns discussed above, it may be appropriate to first determine the institution that is best suited to undertake such a task. While most scholars promote the courts as the appropriate protector of Fourth Amendment rights against encroachment by new technology,[166] others claim that legislatures are best suited for the job.[167] However, while these bodies may be effective to a certain extent, in this instance a large portion of the responsibility will fall on law enforcement and BI[2]Technologies to ensure that the rights of those on whom MORIS is used are protected.[168]

As the ultimate users of the technology, police officers are the first line of defense against abuse of the system. Much of the effort to avoid abuse will need to be made in ensuring that officers apply existing rules regarding stops and fingerprinting to the new technology of iris scanners.[169] In order to ensure a smooth adoption of the technology, police departments and other law enforcement agencies may want to establish explicit rules regarding the proper use of MORIS (or similar devices). In addition to ensuring proper procedure in the use of the iris scanners, police departments will need to be vigilant to avoid abuse through selective use by officers, especially when additional factors, such as racial profiling, appear to currently influence arrest rates.

---

163. *See* Heaton, *supra* note 37.

164. For a broad view of the prevalence of hacking, see the U.S. Department of Justice's 2005 report on cybercrime against businesses. RAMONA R. RANTALA, U.S. DEPT. OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 221943, CYBERCRIME AGAINST BUSINESSES 1 (2005) (noting that, among businesses surveyed, 67% detected at least one cybercrime in 2005).

165. *See* Kate Antonovics & Brian G. Knight, *A New Look at Racial Profiling: Evidence from the Boston Police Department*, 91 REV. ECON. & STAT. 163, 177 (2009) ("[R]esults suggest that preference-based discrimination plays a substantial role in explaining differences in the rate at which motorists from different racial groups are searched during traffic stops.").

166. Levy, *supra* note 46, at 501.

167. *See* Kerr, *supra* note 45, at 806, 838 ("[W]e should not expect the Fourth Amendment alone to provide adequate protections against invasions of privacy made possible by law enforcement use of new technologies."); Levy, *supra* note 46, at 501.

168. *See* Levy, *supra* note 46, at 511–12 (arguing that while law enforcement is best suited to regulate the use of new technologies, it may not have the incentive needed to adequately do so).

169. *See* Smith, *supra* note 3; Albanesius, *supra* note 135.

While safeguarding against abuse will primarily be the responsibility of law enforcement agencies, BI[2]Technologies also bears significant responsibility in preventing misuse of its technology. In order to ensure the accuracy of iris scans by MORIS, BI[2]Technologies could incorporate an error reporting feature into its software that would allow officers to note the existence of false matches as they occur, while still deleting the personal data of those scanned (as they state they already do).[170] In addition to this feature, routine auditing of these error reports, along with testing of the system by an independent party in a real-world setting—preferably by a government oversight or privacy advocacy group—is recommended.

To ensure the security and integrity of data used by MORIS, all information on iris scans sent to and from the iPhones to which the device is attached should be encrypted.[171] Again, this is a function of BI[2]Technologies' software, and as such the company would bear responsibility for this layer of security. In addition to encrypting the data transmitted, the phones will need to be secured against hackers.[172] Apart from the safe use of the system in the field, one would also want to ensure proper storage and oversight of the data collected by MORIS. Currently, the database of iris scans is maintained by MORIS's creator, along with the National Sherriff's Association;[173] however, it would be more prudent to allow independent monitoring, at least, or full ownership, at most, to an organization that is better suited to protect the privacy interests of those whose data is contained in the database. For example, the FBI already maintains such a database for fingerprints and criminal histories, known as the Integrated Automated Fingerprint Identification System (IAFIS),[174] and currently has plans for a replacement of IAFIS that will include iris data.[175] It would be appropriate, and more efficient in the future, to migrate the existing data that MORIS has collected into the FBI database and have one location where all iris information is maintained. In addition to the practical advantages of a single database, giving the FBI control over the iris information could allow them the ability to audit and test MORIS, as mentioned above, as well as the ability to ensure that data of non-criminals is properly deleted after its initial capture. Along with the FBI's efforts, involving an independent government accountability or privacy advocacy group would help to prevent data mining.

---

170. *See Smart phone face scan tech a privacy breach?*, *supra* note 38.

171. *See generally CFNetwork Programming Guide*, APPLE (2011), http://developer.apple.com/library/ios/documentation/Networking/Conceptual/CFNetwork/CFNetwork.pdf (describing iPhone network encryption protocols).

172. *See* Murphy, *supra* note 161.

173. *See* Heaton, *supra* note 37.

174. *See Integrated Automated Fingerprint Identification System*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Apr. 4, 2012). In fact, MORIS uses that database for its fingerprint and facial recognition features. *See* Heaton, *supra* note 37.

175. *See Next Generation Identification*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi-overview (last visited Apr. 4, 2012).

While responsibility for ensuring the proper and safe use of MORIS rests primarily with its creator (BI^2) and users (law enforcement), there are certain steps that a legislature could take to further these goals as well. First and foremost, Congress could pass legislation restricting the use of MORIS without a warrant.[176] It could also pass legislation requiring that the database be handed over by BI^2Technologies to the government, that appropriate oversight be given to an independent group, and that the security features and anti-data mining efforts outlined above are implemented.

IX. CONCLUSION

While MORIS, at least on first impression, raises significant concerns among privacy advocates,[177] given the Supreme Court's current Fourth Amendment jurisprudence, it appears that its proper use by police is constitutional. It is possible, especially given the Court's recent apprehension toward allowing the government unrestricted use of new technologies,[178] that the Supreme Court could adopt a broad interpretation of reasonableness, and declare warrantless mobile iris scans to be a violation of the Fourth Amendment. However, that holding is not likely. So long as proper steps are taken to ensure that the technology is accurate, to safeguard the privacy of iris scan subjects, and to avoid abusive use of the scanners, MORIS (and iris scanning in general) will likely continue to increase in prevalence, and may one day be considered as innocuous to the average citizen as current fingerprinting and DNA identification techniques.

Christopher R. Jones

176. For example, the Electronic Communications Privacy Act of 1986 was enacted in part to restrict the holding of *Smith v. Maryland*, 442 U.S. 735 (1979), which stated that the use of pen registers by phone companies to log one's dialed phone numbers was constitutionally permissible, *id.* at 745–46. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1868–71 (codified as amended in scattered sections of 18 U.S.C.).

177. *See* Howard, *supra* note 54; *Smart phone face scan tech a privacy breach?*, *supra* note 38; Smith, *supra* note 3.

178. *See supra* text accompanying notes 48–52.

*