"The Eyes Don't Lie": Historical, Legal and Policy Considerations Guiding Law Enforcement's Compelled Biometric Identification Practices

Heather M. Patterson

August 2012

WORKING PAPER drafted under the supervision of Professor Paul Schwartz, University of California, Berkeley School of Law

TABLE OF CONTENTS

INTRODUCTION

In November 2010, a small company in Plymouth, Massachusetts unveiled a state-of-the-art law enforcement tool with the dramatic tagline "The Future Has Arrived."[1] Encompassing a pocket-sized high-resolution facial recognition camera, digital fingerprint detector, and iris scanner within a lightweight, portable device designed to be attached an ordinary cell phone, B12's *Mobile Offender Recognition and Information System* (MORIS) resembles a science fiction movie fantasy in function as well as form[2]: It gives officers in the field the unparalleled ability to quickly and accurately crosscheck the identity of broad swathes of persons of interest against a vast, dynamic network of information culled from jail records, criminal histories, and mug shots[3] within multiple jurisdictions from "virtually anywhere, at any time, in a matter of seconds."[4] And if a detainee's face, iris, or fingerprints fail to yield a suitable match, officers can aid future searches by uploading newly acquired information into MORIS's rapidly growing database.[5] Sheriff Paul Babeu of Pinal County, Arizona says, "This technology is futuristic for law enforcement, since a deputy on a rural road can now verify a person's identity even if they provide false name, date of birth or even a fake ID. The eyes don′t lie.″[6]

The technologies underlying MORIS evoke images taken whole cloth from Hollywood-inspired imaginations, but the goal that the device was designed to achieve – to help officers uniquely ascertain human identity by using relatively immutable characteristics of the body – is not new at all. Rather, the identification of individuals via

---

[1] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at time 0:45/7:11, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY (June 14, 2010).
[2] See images of the MORIS device in the Appendix of this paper.
[3] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at times 1:34, 1:51, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY (June 14, 2010).
[4] Sheriff Joseph D. McDonald, Jr., *iPhone for 'The Man': Face-Recognition*, NBC BAY AREA, at http://www.nbcbayarea.com/news/tech/iPhone-for-The-Man-Face-Recognition-Hardware-Available-110965789.html, speaking on video at time 0:47/1:51 (Nov. 29, 2010).
[5] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at time 5:49/7:11, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY (June 14, 2010) (An officer noting, "…the nice thing [about MORIS] is that you can…enroll a person that isn't [yet] in the system.").
[6] Sheriff Paul Babeu, Quoted in Pinal County Press Release, *PCSO Implements New MORIS™ Multi-Modal Biometric Identification System on SmartPhone Units for Deputies*, available at http://pinalcountyaz.gov/Departments/Sheriff/Lists/News/DispFormA.aspx?List=b382d514%2D09a1%2D4490%2D80f0%2D4f0e76b7b4c9&ID=587 (July 18 2012).

their physical characteristics, now called the bread and butter[7] of law enforcement practice, has been the subject of lively technological debates around the world for more than a century.

Sophisticated identification technologies such as MORIS may serve the public interest by reducing fraud, enhancing personal accountability, and improving the physical safety of law enforcement officers and the community.[8] They also have the capacity to serve as a useful government tool for finding, monitoring, and controlling individuals, including those who engage in unpopular political speech.[9] Congressman Al Franken has warned of government face recognition practices generally that they can be used to chill speech by identifying protesters at political events and targeting them for selective jailing and prosecution.[10] And focusing on the storage and distribution of biometric data, the national security counsel for the Electronic Privacy Information Center (EPIC) cautions that biometric data collection and storage raise a host of privacy and civil liberties concerns.[11] Certainly, biometric systems may impose significant social costs. For example, the manner in which biometrics are collected, as well as their differential accuracy, can have a disproportionate effect on particular members of a population, such as minorities, women, and the aged.[12] And the over-collection, over-sharing, and indefinite storage of biometric data can also contribute to the steady erosion of privacy

[7] Nita Farahany, Testimony before the Senate Judiciary Committee Subcommittee Hearing on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties," (July 18, 2012). http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220 (July 18, 2012).
[8] *See* Daniel Solove, *A Taxonomy of Privacy*, 154 U. Pa. Law Rev. 477, 511 (2006).
[9] *Id*. (Citing Richard Sobel, The Degradation of Personal Identity Under a National Identification System, 8 B.U. J. Sci. & Tech. L. 37, 48) (2002).
[10] Senator Al Franken, questioning DOJ Deputy Assistant Director Jerome M. Pender before the Senate Judiciary Committee Subcommittee Hearing on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties" (referencing government materials suggesting that biometrics will be used for chilling speech: "Curiously enough, a lot of the presentations on [face recognition] technology by the Department of Justice show it being used on people attending political events or other public gatherings. I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime — invading their privacy and exposing them to potential false identifications.") (July 18, 2012).
[11] EPIC National Security Counsel quoted in D. Parvaz, *Mobile Biometrics to Hit U.S. Streets*, AL JAZEERA, at http://www.aljazeera.com/indepth/features/2011/07/20117258145965608.html (Aug. 2011).
[12] *See e.g*., Shoshanna Amielle Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity*, ("[B]iometric fingerprint scanners are consistently reported to have difficulty scanning the hands of Asian women, a category not problematized in the scientific literature. Iris scanners exclude wheelchair users and those with visual impairments. More generally, worn down or sticky fingertips for fingerprints, medicine intake in iris identification (atropine), hoarseness in voice recognition, or a broken arm for signature all give rise to temporary biometric failures. More durable failures include cataracts, which makes retina identification impossible or rare skin diseases, which permanently destroy a fingerprint.") (internal citations and quotations omitted) Kindle Locations 146-149, Duke University Press (2011).

rights and expectations, with potentially negative social consequences.[13]

In this paper I adopt MORIS and similar handheld devices as a case study to argue that new prohibitions ought to be placed on police actions in the field, as well as on the contents of linked databases populated by the devices. In Part I, I survey the history of biometric identification practices in America and abroad and situate MORIS within this broader surveillance context. Government use of biometrics is on the rise: The Wall Street Journal[14] and Reuters[15] report that approximately 40 law enforcement agencies across the country, including units in Calhoun County, Alabama, Pinal and Yavapai Counties, Arizona,[16] Pinellas County, Florida,[17] Plymouth County, Massachusetts,[18] and Hampton City, Virginia,[19] use or will soon be using MORIS devices. And although BI2 Technologies reportedly plans to deliver about 1,000 units to law enforcement,[20] it is far from the only portable biometric scanner on the market.[21] Nor is development limited to devices that require the participation of the profiled subject: In the last two years alone, the DOJ's National Institute of Justice has invested in the development facial recognition-enhanced binoculars, investing $1.4 million in technology used to identify people at a distance and in crowds.[22] As Senator Franken observes, "It seems easy to envision facial recognition technology being used on innocent civilians when all an officer has to do is look at them through his binoculars."[23] This is the time to begin seriously addressing legal and policy concerns raised by biometrics writ large.

---

[13] *See* Dan Solove, *Why Privacy Matters Even When You Have Nothing to Hide,* THE CHRONICLE REVIEW, available at *http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/* (May 15, 2011).
[14] Emily Steel and Julia Angwin, *Device Raises Fears of Facial Profiling*, WALL STREET JOURNAL, http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html ("BI2 says it has agreements with about 40 agencies to deliver roughly 1,000 of the devices, which cost $3,000 apiece.") (Aug. 16, 2011).
[15] Zach Howard, *Police to Begin iPhone Iris Scans Amid Privacy Concerns,* REUTERS, http://www.reuters.com/article/2011/07/20/us-crime-identification-iris-idUSTRE76J4A120110720 (July 20, 2011).
[16] *See* CORRECTIONS REPORTER, *Arizona Sheriff to Use Iris Scanners to ID Inmates and Others*, http://www.correctionsreporter.com/2012/02/08/az-sheriff-to-use-iris-scanners-to-id-inmates-others/; http://www.dcourier.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=102947.
[17] *See* Jeff Hughes, *U.S. Law Enforcement Adopting New Smartphone Criminal Recognition Tech*, DIGITAL TRENDS, at http://www.digitaltrends.com/mobile/u-s-law-enforcement-adopting-new-smartphone-criminal-recognition-tech/ (July 13, 2011).
[18] Howard, infra note 16.
[19] *Id*.
[20] Local enforcement agencies get MORIS funds through the U.S. Department of Justice's Office of Community Oriented Policing Services
[21] A list of other portable biometric scanners is included in the Appendix to this paper.
[22] Senator Al Franken, Opening statement before the Senate Judiciary Committee Subcommittee Hearing on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties," (July 18, 2012).
[23] *Id*.

In Part II, I turn to the current Fourth Amendment landscape governing stop and identify statutes, considering their allowable limits in the context of the biometric technologies underlying MORIS and drawing distinctions between the past law enforcement techniques and technologies currently at hand. The guiding question is whether law enforcement's use of MORIS and other biometric identification devices trigger constitutional protections for subjects profiled by law enforcement. Here, I ask (1) under what circumstances are law enforcement officers legally allowed to use MORIS for ascertaining identity; and (2) do, in those allowable circumstances, separate restrictions explicitly or implicitly curtail the use of the fingerprint, face, and iris scanning components of the device? The Supreme Court is unequivocal that detaining a subject under reasonable suspicion that he has committed, is committing, or is about to commit a crime and subsequently asking for his name constitutes a search and seizure deserving of Fourth Amendment protections.[24] But when constructed narrowly, stop and identify statutes pass Fourth Amendment muster, primarily because courts have weighed the benefits of government access to identity more heavily than associated privacy harms to individuals.[25] At the same time, both functional and structural attributes of the MORIS device – for example, their low cost[26] and ease of use, their multi-functionality and automaticity – increase risks to innocent civilians beyond those previously contemplated by courts evaluating the constitutionality of stop and identify statutes.

In Part III, I discuss the implications of large-scale biometric databases. As never before, police are incentivized to detain and question loiterers, the homeless, day laborers, and people who simply don't appear to match their surroundings – by dint, perhaps, of their skin color, language, clothing, or music – and learn who they are and what stories their pasts hold.[27] Once presumed-innocent individuals are detained, police

---

[24] See a discussion of *Hiibel v. Sixth Judicial Dist. Court of Nev*. 542 U.S. 177 (2004) in this paper *infra*.
[25] *Id*.
[26] Each device costs approximately $3,000. Emily Steel and Julia Angwin, *Device Raises Fears of Facial Profiling*, WALL STREET JOURNAL, http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html; *See also* CORRECTIONS REPORTER, *Arizona Sheriff to Use Iris Scanners to ID Inmates and Others*, http://www.correctionsreporter.com/2012/02/08/az-sheriff-to-use-iris-scanners-to-id-inmates-others/; http://www.dcourier.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=102947 ("[MORIS units] will cost the YCSO about $52,000, said [Yavapai County Sheriff's Office Commander John] Russell, and that money is coming from the Jail Enhancement Fund, a discretionary account controlled by the Sheriff. Maintenance and upgrades will run about $9,300 a year.").
[27] *See e.g.*, Franklin E. Zimring, *The City that Became Safe: New York's Lesson for Urban Crime and Its Control* ("The problem with using a predicate offense—alcohol, loud radio noise in a car, marijuana—as a justification for selective enforcement of non-serious crimes is that it really does become the moral equivalent of racial profiling. A much larger

performance of biological 'scans' is humiliating in its public nature: Standing on a street corner while an officer takes high-resolution picture and scans fingerprints surely feels, to the target of the inquiry, far more like events associated with a custodial arrest and booking than does simply providing an officer with one's name. And even if the scans reveal nothing untoward about the detainee and he is free to go, his newly acquired information can be uploaded into interoperable, information-rich databases,[28] thus tagging the individual as suspect in the eyes of society, if not the law.

Finally, in Part IV, I suggest that well-known best practice principles guide the use of MORIS devices now and in the future. The outcome of a legal challenge to law enforcement's use of MORIS is unpredictable. A good result would be for courts to find that compelled identity validation via a biometric device – regardless of biometric modality – impinges upon citizens' constitutional rights against unlawful searches and seizures unless the officer has probable cause to make an arrest. This outcome is unlikely, but possible: Current Supreme Court case law permits state statutes that mandate identity compulsion, but the circumstances under which name information has been contemplated in the past are different from the situations that are present in a MORIS context in a number of respects that I discuss herein. Ill-fitting case law ought not be stretched to allow unfettered biometric identification. But in the absence of a bright-line rule and as a bulwark against abuse, the use of mobile biometric scanners is greatly in need of privacy-protective federal statutory guidance. Without strong situational prohibitions on the devices' use, the potential for overuse causes dignitary harms and may chill speech. Balancing legitimate government interests of officer and community safety against privacy and expressive harms to innocent detainees demands a high standard for use.

BODY-BASED IDENTIFICATION: SCIENCE FICTION OR SCIENCE FACT?

As a class, body-based identification techniques such as face recognition, iris scanning, and fingerprinting are known as *biometrics* – the science of determining or verifying individual identity based on measurements of relatively immutable

---

percentage of African American and Hispanic kids picked up for truancy and curfew will be in the parole, probation, or "criminal record" group….") (Kindle Locations 1904-1910), Oxford University Press (2011).

[28] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at time 5:49/7:11, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY (An officer noting, "…the nice thing [about MORIS] is that you can…enroll a person that isn't [yet] in the system.") (June 14, 2010).

physiological or behavioral characteristics of the person.[29] Although the term feels new, the concept is not. Before the turn of the nineteenth century, French law enforcement officer Alphonse Bertillon promoted more accurate person identification through the field of *anthropometry*,[30] in which measurements and descriptions of components of the human body – including head length and width, facial expressions, gait variations, tattoos, scars, and "the actions and secretions of the organs," were promised to enable human identification with "absolute certainty."[31]

Writing in 1896 in France, Bertillon promised that: "*A sure means of identification would not only have the effect of deterring from crime in general, but would evidently nullify all attempts of whatever kind at a substitution of persons. No impersonations of a pensioner, or a missing heir, or a business man could ever hope to be successful*."[32] Contemporaneously, Britain embraced biometrics via fingerprinting, the then-new technique of logging loops, ridges, and whorls of the fingers endorsed by Sir Francis Galton and British Indian police officer Sir Edward Henry. [33] And in the United States, fingerprinting use rapidly expanded from its initial purpose—monitoring the steady influx of Chinese immigrants into California, particularly in the context of prostitution and sex trafficking – to encompass identification for purposes of civil service exam fraud detection, prisoner identification, soldier differentiation, as well as controlling vagrancy, intoxication, recidivism, and a host of social ills.[34] Perhaps giving credence to Bertillon's early vision of a new social order, New York City magistrate Joseph Deuel noted in the early 1900s, "We are enjoying better order and decorum in the city than ever before, and much of the credit is due to the finger-print process."[35]

Biometric acquisition advancements have proceeded as rapidly as the back-end techniques for storing the massive libraries of information that they generate. Although operating under different names since its establishment by J. Edgar Hoover in 1924, for example, America's National Fingerprint Bureau[36] has grown in size and scope with

[29] Anil K. Jain, Patrick Flynn, and Arun A. Ross. Handbook of Biometrics (pp. 1-2), Springer, 2008.
[30] *See* David Lyon, *Identifying Citizens: ID Cards as Surveillance* at 31, Polity Press, (2009).
[31] Lisa S. Nelson, *America Identified: Biometric Technology and Society* MIT Press (2011).
[32] *Id*. at 32.
[33] *Id*. at 34.
[34] *Id*. (noting the need to distinguish discharged soldiers from deserters and the dead).
[35] *Id*. at 36.
[36] *Id*.

advances in digital processing. Digitization of fingerprints, including flat fingerprint scanning in 1982, digitized rolled impressions in 1988, and electronic submission of fingerprints in 1995, lead to the creation of Integrated Automated Fingerprint Identification Systems (IAFIS).[37] IAFIS is now the world's largest biometric database, with a criminal file with fingerprints, mug shots, height, weight, hair color, eye color, and aliases of 70 million subjects submitted voluntarily by federal, state, and local law enforcement agencies; it also contains a civil file with fingerprints from 31 million federal government employees.[38]

The federal government's newest biometric endeavor is the Next Generation Identification System (NGI)[39] the FBI's enhanced, scalable repository containing ten-print fingerprints and palm prints while enabling easier uploads of a wide variety of official photos and unofficial, publicly-available and user-provided candid snapshots, as well as visual documentation of scars, marks, and tattoos. The NGI is being rolled out in increments: In August 2011, database infrastructure for a Repository for Individuals of Special Concern (RISC) was completed, which allows for nationwide mobile fingerprint identification of "known or appropriately suspected terrorists, sex offenders, and persons of special interest."[40] The summer of 2014 will see the expansion of the national database to include search capabilities for faces, scars, marks and tattoos for investigative purposes, as well as a national "rap back" service enabling notification of the criminal activity of individuals in the database. The following late summer or fall will see the inclusion of iris recognition in the database.[41]

Futuristic uses of biometric are also envisioned. The FBI's Facial Identification Scientific Working Group, for example, is aggressively sponsoring applied research into "universal face and iris workstations," automatic video face detection, technology that will distinguish identical twins, automated retrieval of scars, marks, and tattoos, and

---

[37] *Id*. at 37.
[38] FBI, *Integrated Automated Fingerprint Identification System*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited April 30, 2012).
[39] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi
[40] Jerome M. Pender, Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law, Washington, D.C., at http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties (July 18, 2012).
[41] *Id*.

more. [42] And DARPA is funding active authentication "cognitive footprinting" research that will continuously verify the identity of people as they sit in front of their computer workstations, by detecting unique patterns in keystrokes, eye movements, mouse dynamics, email syntax, reading speed, and more.[43]

Even at a state level, many U.S. states now collect biometric data in their driver's license issuance process to guard against individuals using multiple, state-ID-card-supported identities,[44] or to curb other types of crime.[45] According to a 2012 American Association of Motor Vehicle Administrators (AAMVA) spreadsheet,[46] 34 state DMVs[47] conduct biometric verification with facial images. In Arkansas and West Virginia, facial recognition is mandatory. Additionally, eight states[48] use finger/thumbprint capture. This biometric data collection will help states become REAL-ID compliant, which they are now required to do by January 15, 2013.[49]

Large-scale collections of biometric data are not limited to the United States. Worldwide, the governments of Afghanistan,[50] Brazil,[51] France,[52] India,[53] Liberia,[54]

---

[42] Richard W. Vorder Bruegge, *FBI Facial Recognition and Identification Initiatives*, at http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf at 8.

[43] FBI Broad Agency Announcement, Active Authentication, DARPA-BAA-12-06, available at https://www.fbo.gov/utils/view?id=65da86bb52c0f992d9631447f2a6e357 ("The current standard method for validating a user's identity for authentication on an information system requires humans to do something that is inherently difficult: create, remember, and manage long, complex passwords. Moreover, as long as the session remains active, typical systems incorporate no mechanisms to verify that the user originally authenticated is the user still in control of the keyboard. Thus, unauthorized individuals may improperly obtain extended access to information system resources if a password is compromised or if a user does not exercise adequate vigilance after initially authenticating at the console.") (January 12, 2012).

[44] The AAMVA reports that in Oregon alone between 2008 and 2010, 774 cases were referred to law enforcement. See Biometrics 101: Facial Recognition in Oregon at 18, available at http://www.aamva.org/2011Events/SpringWorkshop/WorkshopDocs/2011WorkshopPresentations/WednesdayApril6/Sarah%20Castner.pdf.

[45] Nominally, these practices are being implemented to curb the enabling of identity theft by catching individuals who juggle more than one identity. They may serve other purposes, however: The impetus for Oregon's program, implemented in 2008, was a package of bills passed in 2005 designed to curb identity theft and methamphetamine use Oregon DMV's facial recognition program hits 1.8 million photos, November 2011, http://www.oregonlive.com/news-network/index.ssf/2011/11/oregon_dmvs_facial_recognition.html ("Pairing biometric data with Oregonians' faces is now a DMV requirement to help battle identity theft. The requirement was part of a package of bills passed in 2005 to stem meth use in Oregon.").

[46] Biometrics in AAMVA community 2012, available at http://www.aamva.org/aamva/DocumentDisplay.aspx?id=%7B259D68E9-F173-4789-8F4B-3395EC7170EC%7D.

[47] Alabama, Arkansas, Colorado, Connecticut, Delaware, the District of Columbia, Florida, Georgia, Hawaii, Indiana, Illinois, Iowa, Kansas, Kentucky, Massachusetts, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Mexico, New York, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Washington, West Virginia, and Wisconsin.

[48] Arkansas, California, Colorado, Hawaii, Mississippi, Oklahoma, Texas, and West Virginia.

[49] Federal Register Volume 76, Number 44, Dept. of Homeland Security at http://www.gpo.gov/fdsys/pkg/FR-2011-03-07/html/2011-5002.htm(March 7, 2011).

[50] FBI, Mission Afghanistan: Biometrics at http://www.fbi.gov/news/stories/2011/april/afghanistan_042911/afghanistan_042911 (April 29, 2011).

Malawi,[55] and Nigeria[56] have recently initiated body-based data collection initiatives in various forms – many with centrally-managed biometrics databases – and for myriad purposes, including establishing automated civil service personnel records, ridding government payrolls of ghost workers,[57] issuing biometric identification cards to government employees, introducing cash transfer systems,[58] or establishing full-scale biometrics-based national identification systems to meet national security[59] or economic and social development needs.[60]

[51] Planet Biometrics, Precise Biometrics Targets Brazil (Oct. 25, 2011), at http://www.planetbiometrics.com/article-details/i/880/.
[52] Angela Daly, "A Time Bomb For Civil Liberties": France Adopts a New Biometric ID Card," Electronic Frontier Foundation Deeplinks Blog (March 8, 2012), at https://www.eff.org/deeplinks/2012/03/french-national-assembly-proposes- new-alarming-biometrics-bill.
[53] Unique Identification Authority of India, at http://uidai.gov.in/.
[54] Jamie Holmes, *I've Got My Eyes on You: How biometric IDs Like Iris Scans will Help Developing Countries Fight Corruption and Bust Fake Workers*, SLATE at http://www.slate.com/articles/technology/future_tense/2011/12/how_biometric_ids_like_iris_scans_will_help_developing_c ountries_fight_corruption_and_bust_fake_workers_.html (Dec. 14, 2011).
[55] Xavier Giné, Jessica Goldberg, and Dean Yang, *Biometric Technology in Rural Credit Markets: The Case of Malawi*, at http://poverty-action.org/sites/default/files/0383%20Malawi.pdf.
[56] Omoh Gabriel, Nigeria: 36 *Govt Organisations Had 43,000 Ghost Workers*, VANGUARD at http://allafrica.com/stories/201107110905.html (July 11, 2011).
[57] *E.g.*. Afghanistan, Liberia, Malawi, and Nigeria. See SLATE at note 49, *supra*.
[58] Alan Gelb and Caroline Decker, *Cash at Your Fingertips: Biometric Technology Transfers in Resource-Rich Countries* at note 3, Center for Global Development, Working Paper 253 (June 2011), available at http://www.cgdev.org/files/1425165_file_Gelb_Decker_biometric_FINAL.pdf ("Countries include: Pakistan, Afghanistan, DRC, Malawi, South Africa, India, Ghana, Namibia, Botswana, Kenya, Nigeria, Iraq, Philippines, Bolivia, and Indonesia.").
[59] Afghanistan.
[60] UIDAI, UIDIA Vision on Micropayments, at http://uidai.gov.in/aadhaar-usage.html (last visited May 1, 2012).

LEGAL PROTECTIONS

Behind concerns about appropriate limits on the collection, use, and distribution of biometric data lie questions about the legal protections currently afforded its targets. In the statutory context, there are few laws that limit how data from a government-run biometric entity can store and use its data. The Privacy Act of 1974[61] provides the framework for most of this regulation, as it requires federal agencies to publish notices of the types of databases it has compiled on individuals.[62] In most circumstances, the Privacy Act provides a statutory right for individuals to access their individual records and begin processes to correct erroneous information.

The Privacy Act, however, has several limitations, including narrow definitions of "records" and "systems of records" that do not cover all government databases or data-gathering activities.[63] For example, although a biometric "record" falls under the Privacy Act by dint of being "*an item…of information about an individual that is maintained by an agency, including, but not limited to, his…criminal…history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph*,"[64] its use is exempt from the Act when the biometric information is gathered by state or local governments, entities that the Act does not regulate. The law also contains numerous exceptions for data gathered for "law enforcement purposes" or put to "routine use."[65] For example, all CIA records are exempt from the Act, as are a number of uses related to national security.

In addition to the Privacy Act of 1974, federal regulations call for agencies to develop Privacy Impact Assessments, which are policies designed to evaluate potential privacy issues that can arise in any government-run database and also offer policies to govern the system's operation and use. To a lesser extent, some state laws provide similar protections.

---

[61] 5 U.S.C. § 552a.
[62] Relevant restrictions in the Privacy Act include limiting the amount of data the agency can collect, 5 U.S.C. § 552a(e)(1) (allowing agencies to store "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"), requiring published notice when they create record systems, 5 U.S.C. § 552a(e)(4), establishing minimum technical safeguards to protect the information, 5 U.S.C. § 552a(e)(10), and providing individuals with a right to access and correct records, 5 U.S.C. § 552a(d).
[63] *See The Privacy Act of 1974*, EPIC, available at http://epic.org/privacy/1974act/ (visited July 30, 2012).
[64] E.g., 5 U.S.C. § 552a(j)(2) and (k)(5) and a(b).
[65] *Id*.

On the whole, however, limited statutory guidance encourages a harder look at Constitutional protections. Thus, more fundamental questions are whether obtaining biological scans via biometric devices such as MORIS constitute protectable searches within the meaning of the Fourth Amendment, and whether courts will likely find these searches to be ones that society regards as reasonable.[66] In *U.S. v. Jones*,[67] the Supreme Court's recent case concerning possible Fourth Amendment protections from the government's prolonged warrantless GPS tracking of a suspected drug dealer, Justice Scalia, writing for the majority, located a different type of technological monitoring – prolonged GPS surveillance via an a device physically attached to the petitioner's car – squarely in the common-law trespassory interest against having one's private property usurped without consent or a valid warrant.[68] However, concurring and dissenting Justices spilled considerable ink discussing technological encroachments upon privacy in the context of the *Katz* test and dynamic social norms. Justice Sotomayor's concurrence emphasized that technological advancements now allow the collection and storage of data that is breathtaking in its scope, permanence, and efficiency,[69] suggesting that the time has now come to reevaluate the third party doctrine:[70] "More fundamentally," she notes, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[71]

---

[66] *Katz v. United States*, 389 U.S. 347 (1967) (where Justice Harlan proposed a two-pronged test to determine when private actions in public places may be constitutionally protected: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy; and second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[67] *United States v. Jones*, No. 10-1259, 2012 BL 14420 (U.S. Jan. 23, 2012).

[68] Id. at 2-10 ("Jones's Fourth Amendment rights do not rise or fall with the Katz formulation…As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates… What we apply [here] is an 18th-century guarantee against un- reasonable searches, which we believe must provide at a minimum the degree of protection it afforded when it was adopted.").

[69] *Jones* (Justice Sotomayor, concurring at 3) ("GPS monitoring… reflects a wealth of detail about…familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility.")

[70] *Id.* at 5.

[71] See also *Smith v. Maryland*, 442 U.S. 735 (1979) (Justices Marshall and Brennan, dissenting) ("But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, ante, at 743, 1 it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a

The dissent similarly focused a large portion of its opinion on the dangers that technological advancements pose, suggesting that because the traditional *Katz* bulwark against privacy invasions (reasonable expectations) are themselves being eroded by increasingly personally-invasive technologies, legislative solutions may be warranted[72]: "A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." In any case, five of the Justices clearly believed that something was terribly amiss with the kind of warrantless high resolution government monitoring that new technology enables.

MORIS and similar devices are unique instantiations of surveillance technology in that they involve the warrantless collection and use biometric data associated with an individual's body, rather than location data associated with an individual's material property. However, the technologically mediated collection of biological images is no less a subject of concern than GPS tracking, and no less in need of legislative action. Congressman Franken, in calling a recent Senate Judiciary Hearing about facial recognition technology, noted that biometric information is unique, permanent, pervasive, and serves as a conduit to a wide variety of information about our lives—including our name, social networking accounts, our locations, and more.[73] Warning that federal privacy laws are "almost totally unprepared to deal with this technology" he suggested that new legislation is needed.[74] As he explained, "unlike what we have in place for wiretaps and other surveillance devices, there is no law regulating law enforcement use of facial recognition technology."[75]

Moreover, constitutional protections may be minimal: Despite sympathetic

---

bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

[72] *Jones* (Justice Alito, concurring in judgment at 13) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.") (Citing Kerr, 102 Mich. L. Rev., at 805–806.).

[73] Senator Al Franken, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties," http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220.

[74] *Id*. ("In the end, though, I also think that Congress may need to act — and it wouldn't be the first time it did. In the era of J. Edgar Hoover, wiretaps were used freely with little regard to privacy. Under some Supreme Court precedents of that era, as long as the wiretapping device did not actually penetrate the person's home or property, it was deemed constitutionally sound — even without a warrant. And so in 1968, Congress passed the Wiretap Act. Thanks to that law, wiretaps are still used to stop violent and serious crimes. But police need a warrant before they get a wiretap. And you can't wiretap someone just because they're a few days late on their taxes — wiretaps can be used only for certain categories of serious crimes. I think that we need to ask ourselves whether Congress is in a similar position today as it was 50 or 60 years ago—before passage of the Wiretap Act.") (July 18, 2012).

[75] *Id*. Emphasis mine.

concurring and dissenting opinions, the *Jones* Court reiterated that the Supreme Court has consistently affirmed its *Katz*[76] holding that what a person knowingly exposes to the public is not a subject of Fourth Amendment protection.[77] But short of wearing a mask, we *must* knowingly expose our biometric information to the public each time we enter the public sphere. As Senator Franken noted, "You can't change your fingerprint, and you can't change your face."[78] Nor can we change, without effort, our voices, heights, footprints, fingerprints, blood type, DNA, or behavioral profiles – all biometric identifiers conceptually akin to faces. And certainly, the Court's reluctance to grant *Katz* protections to biological attributes of the person is not limited to unaided visual senses. In *U.S. v. Dioniso*,[79] for example, the Court noted that "the physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. . . . No person can have a reasonable expectation that others will not know the sound of his voice."

Under the *Katz* Reasonable Expectations of Privacy test, Fourth Amendment doctrine might not be interpreted to cover law enforcement's use of a wide assortment of face recognition technologies. What of other constitutional protections? Perhaps the strongest argument in favor constitutional restrictions on MORIS use is that to successfully acquire personally identifying biological images, officers wielding MORIS technology must at least temporarily detain a subject. The face recognition component of MORIS operates at the distance of approximately five feet, and for best results requires multiple image of the subject acquired from multiple depth-rotated planes of the camera.[80] Thus, an examination of the conditions—and any associated legal protections—under which MORIS images are acquired hits at a middle ground between profiling at a distance and standard police identification practices that occur at the station.

On one end of the continuum, surveillance at a distance, legal scholar Nita Farahany analogizes technologically-mediated face recognition to traditional human

---

[76] Note 60, *supra*.
[77] *California v. Ciraolo*, 467 U.S. 207, 213 (1986); *Florida v. Riley*, 488 U.S. 445, 449-50 (1989).
[78] Franken hearing.
[79] *United States v. Dionisio,* 410 U.S. 1, 14 (1973) ("The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. . . . No person can have a reasonable expectation that others will not know the sound of his voice . . . .")
[80] And iris scanning requires a distance of 6 inches or less. Emily Steel and Julia Angwin, *Device Raises Fears of Facial Profiling*, WALL STREET JOURNAL, http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html

practices of officers scanning a public crowd for faces[81] and again references the third party doctrine: Because the unmediated scan "has never been thought to be a Fourth Amendment search,"[82] the technologically-mediated one should not, either. Rather, she spotlights the behavior of the surveilled *subject*, citing *California v. Greenwood* for the proposition that "when an individual voluntarily forgoes seclusion, he cannot insist that the police avert their eyes."[83] But on the other end of the continuum, station detainments, it may be "routine practice for investigators to collect identifying information from individuals, including their…weight, height, clothing size, shoe size, blood type, and traces of shed DNA,"[84] but much of the case law in this area concerns scientific tests and intrusions into the body *subsequent* to arrest.

Occupying the vulnerable middle ground are temporarily detained subjects who may be less protected from police over-collection by virtue of the less constrained nature of field detainments. Information available about these persons, by virtue of its precision and the scope of associated information available in law enforcement databases, is as revelatory as any information that until recently was only available subsequent to arrest. Thus, a constitutional analysis of MORIS use must take into consideration the reasoning behind law enforcement "stop and frisk" practices, as well as the current allowable scope of those practices – including whether they may plausibly encompass the collection of biometric data that aids identity acquisition. I address this more thoroughly *infra*.

A second argument in favor of constitutional restrictions on MORIS involves the technological nature of the device itself. Although *faces* are plainly visible to officers prior to arrest, some components of MORIS unequivocally rely upon sense-enhancing technology. There is limited Supreme Court precedent that law enforcement use of sense-enhancing technology should be curtailed in some circumstances. In *Kyllo v. United*

---

[81] Nita Farahany, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties," http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220, July 18, 2012. ("[S]earching or seizing a person's likeness by scanning their face from afar does not interfere with their personal security or a right to exclude others they may otherwise enjoy. No physical violence or even physical interference occurs: Mere observation is not tantamount to a search, and certainly not an unreasonable one.").

[82] Nita Farahany, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, "What Facial Recognition Technology Means for Privacy and Civil Liberties," http://www.judiciary.senate.gov/hearings/hearing.cfm?id=daba530c0e84f5186d785e4894e78220 (July 18, 2012).

[83] *Id*.

[84] *Id*. (Citing *Nita A. Farahany, Incriminating Thoughts,* 64 STANFORD L. REV. 351, 368) (2012).

States,[85] the Court invalidated officer's warrantless use of thermal imaging technology to measure heat emanating from a home as evidence of the occupants' use of marijuana-growing lights.[86] By using the thermal reader, a piece of advanced technology "not in general public use," police had violated *Kyllo's* reasonable expectation of privacy and conducted an unreasonable search.[87]

The most obvious candidate for protection under *Kyllo* is MORIS's iris scanning ability. MORIS and other iris scanners take high-resolution photos at a distance of mere inches, enabling the detection of the unique pattern of a detainee's iris, technology for which neither the government or private citizens would consider to be in ordinary public use. Fingerprints occupy a middle ground – they are visible to an officer without aided vision, but without a scanner they are arguably far less useful a tool. On the other hand, the *Kyllo* Court's reluctance to admit infrared evidence of illegal drug growing within a home was grounded as much in the *place* in where the search took place – the privacy of the home – as in in the sensory enhancing technology used to acquire the object of the search.[88] And although Scalia, writing for the majority, "drew a firm line at the entrance of the house," it is far from clear that he would draw a similar line at the entrance of the body, particularly one already under police detainment.[89] And at the rate at which smart phone technologies are becoming less expensive and more available to the public, it is not hard to imagine that in a few short years, biometric scanning technology will be regarded as anything but "advanced." Individuals may not expect to link photos that they take of their friends in public to criminal databases, but they are certainly accustomed to linking them to social networking databases. And private entities such as banks, gyms, and hospitals are already using biometrics to protect themselves— and their customers—

[85] 533 US 27 (2001).
[86] *Id*. at 40.
[87] On the other hand, in *Kyllo v. United States*, 533 U.S. 27 (2001), the Court's reluctance to admit evidence of illegal marijuana growing within a home was grounded as much in the sense-enhancing, advanced imaging device that was used to monitor the thermal radiation as it was in the *place* in where the search took place—the privacy of the home. The Court explained that the determination of whether an expectation of privacy is reasonable is informed by the technology used to gather the information. This was true even though the police observed something in "plain view" from the street, the side of the house.
[88] *Kyllo* ("The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found "it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened.") (citing 476 U.S., at 237, n. 4).
[89] See the brief discussion of DNA and the permissibility of other body samples under *Schmerber* in this paper, *infra*.

from fraud. This widespread adoption of biometrics for purposes of personal identification will only continue to erode the second, objective, prong of the *Katz* privacy test.

Finally, MORIS currently allows officers to easily upload the information of every detainee into a MORIS database, regardless of whether the detainment resulted in an arrest or conviction. In fact, this is seen as one of the perks of the device, [90] and is an incentive for its use.[91] Although this is potentially harmful to subjects, there is little case law that sets structural limitations on the government's storage of detainees for law enforcement purposes. I discuss this more thoroughly *infra*.

Permissible Uses of MORIS to Ascertain Identity in the Field: Detainments

The scope of lawful identity requests where an officer lacks probable cause to make an arrest is today an open question. Two pivotal Supreme Court cases control: *Terry v. Ohio* and *Hiibel v. Sixth Judicial Circuit*. The former allows officers to conduct "stop and frisk" detainments under highly circumscribed circumstances; the latter allows states to criminalize a *Terry* detainee's failure to reply to an identity request.

Scope of Stop & Frisk Searches

The Supreme Court in *Terry* v. *Ohio*[92] provided a narrowly defined[93] exception to the general Fourth Amendment rule that evidence obtained during a search and seizure must be excluded as inadmissible against a petitioner unless the search was predicated on probable cause to arrest.[94] Now, where a reasonably prudent officer is justified in believing that an individual presents a danger to his or others' safety, he may carefully explore the outer surfaces of the person's clothing in an attempt to find weapons, regardless of whether he has probable cause to arrest that individual for a crime.[95]

---

[90] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at time 5:49/7:11, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY, June 14, 2010 (An officer noting, "…the nice thing [about MORIS] is that you can…enroll a person that isn't [yet] in the system.").
[91] The database appears to be small at this point – quote here.
[92] 392 U. S. 1 (1968).
[93] *Id*. at 16 ("Given the narrowness of this question, we have no occasion to canvass in detail the constitutional limitations upon the scope of a policeman's power when he confronts a citizen without probable cause to arrest him.").
[94] *Id*. at 20 ("We do not retreat from our holdings that the police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure") (citing *Katz v. United States*, 389 U.S. 347 (1967); *Beck v. Ohio*, 379 U.S. 89, 96 (1964); *Chapman v. United States*, 365 U.S. 610 (1961)).
[95] See Franklin E. Zimring, *The City that Became Safe: New York's Lessons for Urban Crime and Its Control* (Kindle Locations 1890-1894), Oxford University Press (2011).

In *Terry*, an observing officer hypothesized that three men were contemplating and planning a daylight robbery of a store. Believing that swift action was needed to ensure the safety of the populace, but lacking probable cause to arrest, the officer detained the men and conducted a brief pat down of their outer clothing to determine whether they were armed. His efforts revealed that one of the men was carrying a handgun, which was subsequently admitted as evidence in the trial against him. The detainee objected on grounds that the gun was obtained during a warrantless search and seizure of his person and was therefore constitutionally inadmissible under the Fourth Amendment under the exclusionary rule.

On the initial issue of whether the officer's conduct was governed by the Fourth Amendment, the Supreme Court emphatically rejected the argument put forth by the State that the officer's "stop and frisk" did not constitute a seizures or search – rather, Justice Harlan in his majority emphasized that "whenever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person." Moreover, "it is nothing less than sheer torture of the English language to suggest that a careful exploration of the outer surfaces of a person's clothing all over his or her body in an attempt to find weapons is not a 'search.'"[96]

Rather, the Court concentrated its analysis on the need for and reasonableness[97] of of the officer's conduct, "both at…inception and as conducted."[98] Because the officer was able to point to "specific and articulable facts" that bolstered the claim that an important government interest was at hand (here, the unusual 'casing' behavior of the suspects coupled with the necessity of assuring himself that the detainee is not "armed with a weapon that could unexpectedly and fatally be used against him"),[99] and because that

[96] *Terry v. Ohio* at 16-17 ("There is some suggestion in the use of such terms as "stop" and "frisk" that such police conduct is outside the purview of the Fourth Amendment because neither action rises to the level of a "search" or "seizure" within the meaning of the Constitution. We emphatically reject this notion. It is quite plain that the Fourth Amendment governs "seizures" of the person which do not eventuate in a trip to the stationhouse and prosecution for crime -- "arrests" in traditional terminology. Moreover, it is simply fantastic to urge that such a procedure performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a 'petty indignity.' It is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly.").

[97] *Elkins v. United States*, 364 U.S. 206, 222 (1960) "What the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures."

[98] *Terry* at 19-20 ("And, in determining whether the seizure and search were "unreasonable," our inquiry is a dual one -- whether the officer's action was justified at its inception, and whether it was reasonably related in scope to the circumstances which justified the interference in the first place.")

[99] *Id*. at 24 ("We cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest.").

interest outweighed the minimally intrusive nature of the search conducted by the officer (patting down clothing in a search for weapons, rather than a general exploratory search for evidence of criminal activity), [100] the conduct was deemed constitutionally allowable.

Scope of State Stop & Identity Statutes

Importantly, *Terry* provides the legal foundation for a host of state law "stop and identify" statutes that allow officers who have temporarily detained a subject under *Terry* to also ask for his name. At least 23 states currently have stop and identify statutes.[101] In all cases, these laws allow an officer to ask for identity "whenever there is reasonable ground [particularized suspicion] to suspect that he is committing, has committed or is about to commit a crime" if the request for identity has an immediate relation to the purpose, rationale, and practical demands of [the] stop. They also criminalize a subject's failure to identify himself. About half of states with stop and identify statutes require that detainees, if asked, provide an address and a credible account of their presence at that location, as well as a future purpose or destination.[102] These statutes are based on the Uniform Arrest Act[103] or the Model Penal Code.[104]

Other states, including Nevada, and Ohio, specifically protect detainees from this requirement, typically specifying that a detainee shall not be compelled to provide any information beyond his name and address. And the remainder of states is more protective of detained suspects, merely making it unlawful to provide *false* identification to an officer or to fail to provide identity *subsequent to arrest*. In Texas, for example, a bill requiring that a subject detained under Terry identify himself upon penalty of arrest, SB 843, died in the House in 2011.[105]

---

[100] *Id*. at 28 ("The manner in which the seizure and search were conducted is, of course, as vital a part of the inquiry as whether they were warranted at all.")

[101] A list of stop and identity statutes, with relevant language, is included in the Appendix to this paper.

[102] Stop and identify laws are a departure from more restricted state statutes merely making it unlawful to provide *false* identification to an officer or to fail to provide identity *subsequent to arrest*. In Texas, for example, where a bill requiring that a subject detained under Terry identify himself upon penalty of arrest, SB 843, died in the House in 2011. See http://www.legis.state.tx.us/BillLookup/History.aspx?LegSess=82R&Bill=SB843.

[103] The Uniform Arrest Act, 28 Va. L. Rev. 315, 344 (1942) (permitting an officer to stop a person reasonably suspected of committing a crime and "demand of him his name, address, business abroad and whither he is going.").

[104] Model Penal Code. See ALI, Model Penal Code, §250.6, Comment 4, pp. 392—393 (1980) (providing that a person who is loitering "under circumstances which justify suspicion that he may be engaged or about to engage in crime commits a violation if he refuses the request of a peace officer that he identify himself and give a reasonably credible account of the lawfulness of his conduct and purposes.").

[105] http://legiscan.com/gaits/text/235447

History and Rationale of State Stop and Identify Statutes

In considering whether state stop and identify statutes would likely be constitutionally permitted to encompass biological image acquisition via a MORIS device during a *Terry* stop, it is important to understand the evolution of the Court's reasoning on identity acquisition, generally. In 1967, Justice White's *Terry* concurrence suggested that although detainment itself justified the protective frisk for weapons because officers could be injured during the course of keeping a suspect detained, detainees were *not* compelled to actually answer any questions directed to him by an officer: "[G]iven the proper circumstances, such as those in this case, it seems to me the person may be briefly detained against his will while pertinent questions are directed to him. *Of course, the person stopped is not obliged to answer, answers may not be compelled, and refusal to answer furnishes no basis for an arrest.*"[106] Moreover, in the year following *Terry*, the Court in *Davis v. Mississippi* further reiterated the "settled principle" that [officers] have no right to compel [temporary detainees] to answer voluntarily questions.

Surprisingly, though, in coming years the Supreme Court twice declined to rule on the issue explicitly, and then took a very different approach, favoring law enforcement interests over those of detainees. First, in *Brown v. Texas*[107] in 1979, the Court said that it "need not decide whether an individual may be punished for refusing to identify himself in the context of a lawful investigatory stop which satisfies Fourth Amendment requirements," because the issue before the Court there was whether the stop itself was based on reasonable suspicion. In 1983 in *Kolender v. Lawson*,[108] the Court held a California stop and identify statute void for vagueness but did not subject it to Fourth Amendment analysis.

But lower courts were split: The Ninth Circuit in *Carey v. Nevada Gaming Control Bd*[109] in 2002 took the position that because the Supreme Court had not reversed the Ninth Circuit's alternate holding, in *Kolander v. Lawson*, that compelled self-

[106] *Terry* (Justice White concurring at 31).
[107] 443 U.S. at 53 n. 3.
[108] 461 U.S. 352, 361-62 n. 10 (1983) ("Because we affirm the judgment of the court below on this ground, we find it unnecessary to decide the other questions raised by the parties because our resolution of these other issues would decide constitutional questions in advance of the necessity of doing so.").
[109] 279 F.3d 873 (9th Cir. 2002).

identification violates the constitution, this holding was still good law.[110] It had also relied on *Lawson* in reaching the same conclusion in *Martinelli v. City of Beaumont* in 1987.[111] However, the Tenth Circuit in *Oliver v. Woods* in 2000[112] reached a different conclusion, noting that the criminality of a failure to respond is an open question, that because the Supreme Court had declined to rule on the issue and "because the initial stop was [lawfully based on reasonable suspicion of criminal activity], Mr. Oliver had no clearly established constitutional right to *refuse* to identify himself and to terminate the encounter."[113] Thus, what the Ninth Circuit interpreted as a tacit endorsement of its own prior ruling, the Tenth apparently interpreted as the Court's unwillingness to overrule state authority.

Not until three years after September 11, 2001 did the Supreme Court finally carve out an exception to its previously alluded to "settled principle" of a detainee's right to not respond to an officer's questions about identity and resolve the issue in favor of compulsory self-identification. In *Hiibel v. Sixth Judicial District Court of Nevada*,[114] the Court considered the constitutionality of a Nevada state law mandating identity disclosure during *Terry* stops. A Humboldt County Nevada Sheriff's Deputy had temporarily detained the petitioner[115] as he was parked, haphazardly, alongside the road; because of a prior tip and the unusual circumstances of the parked car and its animated occupant, the officer suspected Hiibel of striking his daughter and of driving while intoxicated. As part of his efforts to understand the circumstances at hand, the officer asked Hiibel for identification. After Hiibel steadfastly refused to identify himself, declining the officer's request for identification eleven times,[116] the officer arrested

---

[110] *Id*. ("In *Kolender v. Lawson*, 461 U.S. 352, 361-62, 103 S.Ct. 1855, 75 L.Ed.2d 903 (1983), the Supreme Court affirmed our decision on the ground that the statute was void for vagueness and declined to address our alternate holding that the statute also violated the Fourth Amendment. Nevertheless, the Supreme Court did not reverse our decision in Lawson; therefore, Lawson' s holding that the police cannot, consistent with the Fourth Amendment, compel identification during an investigatory stop remains good law in this circuit.")

[111] 820 F.2d 1491, 1494 (9th Cir. 1987).

[112] 209 F.3d 1179, 1190 (10th Cir. 2000).

[113] Id. (emphasis mine). The court continues: ("Even though the record indicates Officer Woods no longer suspected Mr. Oliver of illegal oil dumping, trespass, or any other illegal act in the parking lot connected to his original suspicion of criminal activity, Officer Woods could have reasonably believed he had probable cause to arrest Mr. Oliver for violating [the stop and identify statute] when Mr. Oliver refused to identify himself and left the parking lot.").

[114] *Hiibel v. Sixth Judicial Dist. Court of Nev*. 542 U.S. 177 (2004).

[115] Larry Hiibel's accounting of events can be viewed at http://papersplease.org/hiibel/.

[116] For an account of the facts of the case, see http://www.nevadajudiciary.us/index.php/supnews/78-us-supreme-court-opinion-in-hiibel-vs-state-of-nevada.

Hibbel on authority of a Nevada statute[117] which allowed, but did not require, police to *"...detain any person whom the officer encounters under circumstances which reasonably indicate that the person has committed, is committing or is about to commit a crime…only to ascertain the person's identity and the suspicious circumstances surrounding the person's presence abroad.*" Hiibel, who was fined $250, challenged the constitutionality of the Nevada law, arguing in part that it allowed officers to circumvent the probable cause requirement and arrest a person for merely being suspicious.

Writing for the majority, Justice Kennedy resolved the issue by heavily favoring government interests – the benefit to officers and community safety in an officer's demand for a detainee's identity – against the intrusion caused by asking a subject to identify himself. "Identity," the majority reasoned, helps a law enforcement officer know whether a suspect is wanted for another offense or has a record of violence or mental disorder, and may be needed to "assess the situation, the threat to [officers] own safety, and possible danger to the potential victim."[118] On the other hand, the request for a name doesn't fundamentally change the location or the duration of a *Terry* stop, the type of factors that the *Terry* Court had considered when contemplating potential harms to detainees.[119] Thus, a properly narrow and precise state law statute may permit officers who detain a suspect during the course of a lawful *Terry* stop to ask the suspect for his name upon threat of criminal penalty for failing to comply, so long as "the request for identity has an immediate relation to the purpose, rationale, and practical demands of [the] stop," and the statute itself clearly instructs how the subject may satisfy the officer's request.[120] Thus, where a stop and frisk detainment is based on specific, objective facts establishing reasonable suspicion to believe the suspect was, is, or will be involved in a crime, an officer may ask the detainee's name, and if he does, the detainee must provide it.

---

[117] Nevada Revised Statute 171.123, 2010 update available at http://law.justia.com/codes/nevada/2010/title14/chapter171/nrs171-123.html.
[118] *Hiibel* at 186 ("Officers called to investigate domestic disputes need to know whom they are dealing with in order to assess the situation, the threat to their own safety, and possible danger to the potential victim.").
[119] *Id.* ("On the other hand, the Nevada statute does not alter the nature of the stop itself: it does not change its duration or its location") (internal citations omitted); *Terry v. Ohio* ("This Court has held, in the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope.").
[120] *Hiibel,* 542 U.S. at 188.

Application of Terry and Hiibel to MORIS

The Court's *Hiibel* opinion changed the course of the line of concurring opinions and dicta that had indicated that individuals were not obligated to answer questions, including questions about identification, in the absence of an officer's probable cause for arrest. Notably, in considering potential harms to a potential detainee, the majority focused more on the purpose of the request, the narrowness of the statutory language, and the inconvenience that the detainee might suffer than on the potential for police abuse, or the dangers of vast government databases filled with information, to which identity is a conduit. In particular, the Court dealt very lightly with the practical issue of officers being tempted to manufacture a connection between circumstances of the stop and the information requested, particularly to obtain information from minorities. Because the Nevada statute required an immediate nexus between the purpose of the stop and inappropriate requests for identification upon threat of penalty, the Court suggested that the threat of misuse was properly minimized.[121]

The practical outcome of *Terry* and *Hiibel* has been both positive and discouraging: On the one hand, crime in New York City, where officers actively conduct aggressive protective stops, has dropped dramatically[122] as stop and frisk tactics have increased.[123] Experts speculate that the stop and frisks play a role in that decline.[124] As legal scholar Frank Zimring notes, "The two important tactical measures that almost certainly reduced crime in New York City were (1) the emphasis on hot spots for enforcement, aggressive street intervention, and sustained monitoring; and (2) the priority targeting of public drug markets for arrest, surveillance, and sustained attack."[125] On the other hand, evidence is also now coming to light that *Terry* stop and frisks disproportionately affect minorities. In New York City, for example, police made nearly

[121] *Id*. ("…the threat of criminal sanction helps ensure that the request does not become a legal nullity.").
[122] Zimring at Kindle Locations 72-76 ("The average city's crime rate decline hovered around 40% and stopped in 2000. The New York City decline has so far lasted twice as long, and the average rate drop is also twice as large. Rates of homicide, robbery, and burglary have dropped over 80% in 19 years. Auto theft has dropped 94%. Are these official statistics accurate? If so, it would be the largest crime drop ever documented during periods of social and governmental continuity. By 2009, the homicide rate in New York, which had been over 30 per 100,000 in 1990, had dropped to under 6 per 100,000, a rate lower than the city enjoyed in 1961.").
[123] Id. ("The volume of official stop reports increases from 41,438 in 1990 to 581,382 over the two decades covered, a 14-fold increase.").
[124] See e.g., Zimring Chapter 5, discussing increases in police patrols, particularly during times "when 'the bad guys' were at work" and uses of stops and arrests as preventative enforcement against those bad guys.
[125] Zimring at Kindle Locations 2298-2300.

700,000 stops in 2011; about 85 percent involved blacks or Hispanics.[126] As a 44-year-old Bronx resident recently pointed out to the New York Times, "You know it's excessive when you see people get stopped who really don't deserve to be stopped, like kids going to school. The police just jump out, stop them, search them, take their names down, then get back in their car and leave, and the kids don't know what went on."[127]

What result for MORIS? *Hiibel* may – unfortunately – have cleared the path for officers to request additional information during the course of *Terry* stops, and for them to use means other than merely "asking" to force detainees to respond. In his *Hiibel* dissent, Breyer asks a prescient question: whether, in contravention of settled precedent permitting a detainee to remain silent about his identity, "a State, in addition to requiring a stopped individual to answer 'What's your name?' [will now] also require an answer to 'What's your license number?' or 'Where do you live?'" His concerns appear to have come to pass, at least for now. As noted *supra*, more than half of state stop and identify statutes that criminalize failure to respond also now include a provision that an officer may inquire as to a detainees purpose for being in a given location, and many also require detinees to explain their future plans to officers. In 2007, the DC Circuit in *United States v. Askew* allowed police conducting a *Terry* detainment to unzip the detainee's outer coat in order to allow the victim of a robbery to see whether the detainee was a blue sweatshirt that the victim recognized. The court reasoned "if the police during a *Terry* stop may take fingerprints for identification purposes [discussed *infra*], it logically follows that the police…may unzip an individual's outer jacket for identification purposes." And in *Arizona v. United States* in 2012,[128] the Supreme Court upheld a new identification provision of the controversial SB 1070, allowing state officers to make a "reasonable attempt" to determine immigration status during the course of "an authorized, lawful detention." MORIS inquiries, which yield for now a subject's name and associated criminal history, could be viewed as consistent with government interests in protecting the officer and society, and even less privacy invasive than forcible roadside undressing or immigration checks.

---

[126] Michael M. Grynbaum and Marjorie Connelly, Majority in City See Police as Favoring Whites, Poll Finds, NEW YORK TIMES, available at http://www.nytimes.com/2012/08/21/nyregion/64-of-new-yorkers-in-poll-say-police-favor-whites.html?pagewanted=all (Aug. 20, 2012).
[127] *Id*.
[128] 567 U. S. ____ (2012).

But although state statutes have become more expansive than the language of *Hiibel* allows, they may have done so impermissibly, straying from Supreme Court teachings over time. In the context of *Terry* stops, legal scholar David A. Harris points out that "perhaps as a result of the high-visibility of use of frisks as a contemporary crime control device, or because of general public antipathy to crime, lower courts have stretched the law governing frisks to the point that the Supreme Court might find it unrecognizable. When confronted with [certain types of situations or persons], police [might] automatically frisk, whether or not any individualized circumstances point to danger." Even Justice Kennedy writing for the Court in *Arizona v. United States* cautioned that the immigration status provision might "raise constitutional concerns" as applied, and suggested that it could be subject to constitutional challenges after it goes into effect.[129]

To clarify, it is important to look at what the Court originally allowed under *Terry* and *Hiibel,* and why. Where an officer does not have probable cause for arrest, *Hiibel* allows a state to compel a detainee's *self-disclosure* of his *name* so long as "the request for identity has an immediate relation to the purpose, rationale, and practical demands of [the] stop." The *Hiibil* Court particularly noted that the constitutionality of the Nevada stop and identify statute hinged on its being narrow and precise in its requirement that a suspect "only…disclose his name,"[130] via a means chosen by the suspect: "As we understand it, the statute does not require a suspect to give the officer a driver's license or any other document. Provided that the suspect either states *his name* or communicates it to the officer by other means — *a choice, we assume, that the suspect may make* — the statute is satisfied and no violation occurs." Thus, the Nevada statute was held to be lawful in part because of the boundaries it carefully placed on the content of the exchange between the officer and detainee. And as with *Terry*, the purpose of the request is to ensure the officer's safety. The Supreme Court in *Michigan v. Long*[131] noted that "a *Terry* investigation, such as the one that occurred here, involves a police investigation 'at close range,' when the officer remains particularly vulnerable in part because a full custodial

[129] *Id*.
[130] Citing 118 Nev., at 59 ("The suspect is not required to provide private details about his background, but merely to state his name to an officer when reasonable suspicion exists.").
[131] 463 U.S. 1032 (1983).

arrest has not been effected, and the officer must make a quick decision as to show to protect himself and others for possible danger."

State statutes that allow officers seemingly unfettered access to information about a detainee thus go beyond *Hiibel* and *Terry's* specifications and purpose; to further allow the use of biometric scanning to acquire that information would arguably distort them impermissibly in several ways. First, in using MORIS – whether the face print, fingerprint, or iris scan component – an officer is forcibly 'taking' something from the detained, rather than receiving it volitionally from him. This alters the locus of control from the detainee (self-disclosure) to the officer. Although a self/other distinction may not be glaringly constitutionally relevant, it certainly implicates different privacy interests than the Court contemplated in *Hiibel* and goes instead to the indignity of the practice itself – the heightened scrutiny paid to a subject that is ordinarily reserved for humiliating police station and prison practices. In its very physicality, the officer-directed MORIS scan practice is more like *Terry* stop and frisks than a verbal name requests. Making a detainee remain stationary an officer's watchful eye while images are taken of various parts of his body is conceptually and physically far more similar, to both the officer and suspect, to patting down someone's outer person than merely listening to him speak his name aloud. The harm that the *Terry* Court contemplated in protective stops wasn't only the invasiveness of the physical touching itself; it was also the embarrassment of standing in public while subjected to an officer's actions, looking and feeling like a criminal in the eyes of oneself, society, and the law: "It is simply fantastic to urge that [frisks] performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a 'petty indignity.' It is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly."[132] And in contemplating onsite fingerprinting in the absence of probable cause for arrest, Justices Brennan and Marshall in *Hayes v. Florida* reflect on dignitary harms that onsite fingerprinting would cause detainees, noting that the practice, which would be "apparently undertaken in full view of any passerby," "would involve a singular intrusion on the suspect's privacy."[133]

[132] *Terry* at 16-17.
[133] 470 U.S. 819 (1985).

Second, the government interest served by *Terry* and *Hiibel* was mitigation of immediate harm to the investigating officer by allowing a limited search (outer clothing) for a limited item (weapons) for a limited purpose (safety) where time was of the essence. Detainment itself was the situation that justified the frisk: the Court considered it unduly harmful to an officers to require him to stand by and monitor a suspect while not knowing whether he was in danger of being shot or stabbed. But the purpose of onsite biometric scanning goes well beyond assessing identity to preserve an officer's safety in the moment. As Justices Brennan and Marshall note in concurrence in *Hayes v. Florida*, hypothetical onsite biometric sampling would likely fail under *Terry*, primarily because "an intrusion…would not be justifiable as necessary for the officer's protection."[134]

Not only does the intent behind biometric scanning not meet the *Hiibel* criteria that a request for identity be tied to the crime that the subject is suspected of "having been involved with, being involved with, or going to be involved with," it allows for an expansion amounting to a fishing expedition for past infractions. For instance, MORIS can be used to run a background check on a suspect to link him with crimes already committed, either by seeing if he matches a list of sex offenders or parolees. But it can also be integrated with federal, state, and local databases[135] and used to assess whether a fingerprint matches a latent, unsourced crime scene print, and in theory, can link to FBI or DOJ linked databases that themselves could put flags out for a variety of behaviors – including information acquired from private sources about religion or political preferences. Indeed, there are currently no stated limits on what a MORIS database could contain. Thus, to allow MORIS use under *Hiibel* is to provide is a procedurally backward loophole that does not improve officer safety in the moment but that encourages an abuse of power: Officers may, under this view, temporarily detain a person without probable cause for arrest and use a 'name verification' technology to gather far more information about the suspect than a name, and indeed far more than would ordinarily be available

[134] 470 U.S. 819 ("It would seem that on-site fingerprinting (apparently undertaken in full view of any passerby) would involve a singular intrusion on the suspect's privacy, an intrusion that would not be justifiable (as was the pat-down in *Terry*) as necessary for the officer's protection. How much time would elapse before the individual would be free to go? Could the police hold the individual until the fingerprints could be compared with others? The parties did not brief or argue these questions, the record contains nothing that is useful in their resolution, and (naturally enough) the courts below did not address them.").

[135] B12 Technologies, *MORIS Handheld Iris/Face/Fingerprint Biometric Recognition Device*, YOUTUBE, text on video at times 1:34, 1:51, at http://www.youtube.com/watch?feature=player_embedded&v=jk-NL71IwjY (June 14, 2010).

without a trip to the police station. And this is exactly the harm that the government should seek to avoid – detaining someone on a flimsy pretext, then scanning them and using the acquired information in conjunction with that behavior to manufacture probable cause.

Third, an absence of clear limitations on MORIS use will contribute to justifiable police confusion about permissible data collection standards and practices. In Breyer's *Hiibel* dissent, he asks "can a police officer, who must know how to make a *Terry* stop, keep track of the constitutional answers [regarding what he is allowed to ask a detainee]?" Preliminary evidence suggests that police officers may not always be able to keep track of the constitutional answers even now, before widespread MORIS use. Stepping back from MORIS and looking only at the application of stop and identify statutes generally, there seems to be substantial confusion among personnel on the ground as to who may be asked to provide identification, and under what circumstances.[136]

There is wide disparity in how officers view MORIS and how they plan to apply it. Some officers do seem to be erring, appropriately, on the side of conservative application of the techniques. For example, Sheriff Paul Babeu recently said that, ″we currently use the [i]ris technology to positive ID…in patrol…any suspects and those arrested for crimes.," and assured that "it will be used with consent, or when we have *lawful probable cause* for criminal offenses." Sheriff Joseph McDonald Jr. of Plymouth County, Massachusetts, assures that "two hundred years of constitutional law isn't going away,"[137] but plans to tell deputies that *reasonable suspicion* is necessary to use the facial recognition component of MORIS. And Brockton, Massachusetts Chief William Conlon seemingly sets the bar just above dragnet surveillance when he says "We're not gonna just *randomly stop people randomly on the street* and ask to take their picture."[138] As he notes, "It is just a picture. If you are out in public, I can take a picture of anybody."[139]

---

[136] *See e.g.*, http://forums.officer.com/t83424/ (in which officers argue amongst themselves about whether passengers in cars lawfully detained are subject to Fourth Amendment protections against search and seizure, and particularly whether they, like the driver of the car, must provide identity information upon request).

[137] Comments to article "Surveillance State Tactics Increasing: Police Starting to Use Facial Recognition Devices" NAKED CAPITALISM at http://www.nakedcapitalism.com/2011/07/surveillance-state-tactics-increasing-police-starting-to-use-facial-recognition-devices.html#2Eky6WS7h7r38Ogz.99 (July 13, 2011).

[138] ___ (video citation).

[139] http://www.nakedcapitalism.com/2011/07/surveillance-state-tactics-increasing-police-starting-to-use-facial-recognition-devices.html

Perspectives from officers and others weighing in anonymously online run the gamut. One notes that "I can see the future where you will be required to read a MIRANDA type warning to someone before you can take a picture of their eyes…If used sparingly [current practices] will fly for quite awhile but you know there are some [officers] among us who will not use it sparingly and then the new laws will come down on us all. *It will all come down to having [probable cause] or not...*"[140] Perhaps this cautious officer contemplates colleagues like the following, who expresses enthusiasm for the device's seemingly less stringent use requirements: "How many times have you had to let someone go on their way, because you couldn't prove they were not who they claimed to be *and you had no [probable cause]* to take them to the station? Usually it's a passenger on a car stop, or someone in the crowd at a bar fight (who didn't see nuthin). Then later you found out the guy was a parolee at large. [MORIS] should be praised by Homeland Security."[141]

Chief William Conlon of the Brockton, Massachusetts Sheriff's department, quoted *infra*, intimates that MORIS is primarily a time-saving device that improves law enforcement efficiency – rather than bringing a suspect back to the station for criminal background checks, the necessary information can be gotten in the field. "This is something that the officers can actually use when they're out on the road," says Chief Conlon in a video interview, "so they don't have to rely on bringing somebody back here to figure out who they are." Online commenters agree: I think it will save people the trouble of having to go to jail just to be identified. A great time saving device."[142] These comments imply, of course, that officers would have probable cause to bring suspects into the station in the first place. They can be taken at face value, or they can be understood more cynically to mean that MORIS will save officers the trouble of manufacturing probable cause to take suspects to the station.

It's possible that until laws are clearer, leadership will guide use. But leadership

[140] Internet user k9hanir, available at http://www.policeone.com/police-products/investigation/cameras/articles/3989008-New-police-iPhone-facial-scanner-promising-and-controversial/ (July 14, 2011 at 3:30PM).
[141] Internet user sarge889, available at http://www.policeone.com/police-products/investigation/cameras/articles/3989008-New-police-iPhone-facial-scanner-promising-and-controversial/ (July 14, 2011 11:52AM).
[142] Internet user j794, available at http://www.policeone.com/police-products/investigation/cameras/articles/3989008-New-police-iPhone-facial-scanner-promising-and-controversial/ (July 14, 2011 09:32AM).

acknowledges widespread confusion and concern: Director of public information and technology at the Plymouth County Sheriff's department admitted that he didn't know when officers would be issued guidelines on MORIS use, or what those guidelines would say. He acknowledges that "nobody wants to make a bad arrest, nobody wants to violate anyone's rights," but says, "I'm dancing on the head of a pin here because I'm not a constitutional scholar."[143]

Certainly, if an officer can meet a probable cause standard, his onsite use of MORIS is far more likely to be legal under current regimes. It is now becoming more common for officers to collect a vast amount of information about a suspect even prior to conviction. For example, federal law mandates that any individual who is "arrested, facing charges, or convicted," or "on release, parole, or probation," or already in the government's DNA CODIS database may be detained, restrained, and compelled by the U.S. Attorney General, the Director of the Bureau of Prisons, or federal probation officers and compelled to provide a "tissue, fluid, or other bodily sample." The Director of the FBI, "shall carry out a DNA analysis on each such DNA sample and include the results in [the FBI's] CODIS database" without a warrant.[144] A similar California initiative, Proposition 69, also requires the warrantless collection of DNA from felony arrestees. This initiative expands the previous rule — that collection of DNA from presumptively innocent people was not appropriate — to persons merely arrested, but not convicted, of felony. The Ninth Circuit has recently upheld the legality of this practice under the Fourth Amendment.[145]

Onsite Fingerprinting and Other Biometric Modalities

Comments above suggest that in the absence of probable cause (or clear statutory guidance), officers' use of the MORIS device will likely be shaped by the specific information that the device is used to collect. Although legal standards for two MORIS

[143] D. Parvaz, Mobile Biometrics to Hit U.S. Streets, at http://www.aljazeera.com/indepth/features/2011/07/20117258145965608.html (Aug. 2011).
[144] 42 USC § 14135a, Collection and use of DNA identification information from certain Federal offenders, available at http://www.law.cornell.edu/uscode/text/42/14135a.
[145] *Haskell v. Harris*, 2012 WL 589469 (9th Cir. Feb. 23, 2012). And see *United States v. Fricosu (*Fricosu challenged the constitutionality of the DNA collection incident ot arrest on Fourth Amendment grounds; Colorado District Judge Blackburn denied the motion, available at http://www.genomicslawreport.com/wp-content/uploads/2012/04/US-v-Fricosu-Order.pdf); But c.f. *In re Welfare of M.L.M. and State v. Johnson* (rejecting challenges of DNA Fingerprinting based on 4th Amendment and Equal Protection grounds).

modalities, onsite facial and iris scanning, have not been discussed by courts, onsite fingerprinting conducted by law enforcement in the absence of probable cause has acquired a more prominent position through dicta suggesting that the Court may view favorably the government collection of fingerprints from temporary detainees. In the leading case on the constitutionality of fingerprinting outside of the context of an arrest, *Hayes v. Florida*,[146] the Supreme Court held that probable cause was required to transport a person from his home to a police station in order to fingerprint him. In that case, a suspected rapist initially refused to be fingerprinted after police confronted him on his doorstep and asked that he submit his prints, but relented when the officers threatened to arrest him. However, because the officers actually lacked probable cause for an arrest, they simply drove the man to the police station and collected his fingerprint evidence there, claiming that the suspect's 'consent' to be driven to the station dispensed with any warrant requirement. The Court ruled the resulting fingerprint evidence inadmissible, clarifying that "a suspect may not be apprehended, detained, and forced to accompany the police to another location to be fingerprinted without a warrant or probable cause. The intrusion on the suspect's freedom of action in such a case is simply too great to be "reasonable" under the Fourth Amendment."

The Court thus affirmed its prior holding in *Davis v. Mississippi* that the scope of information that can be lawfully acquired during detainments at police headquarters without probable cause extend to fingerprinting. The Court's reasoning in *Davis* was clear: First, fingerprints themselves are the type of information that the Fourth Amendment protects, because they provide officers "something of evidentiary value."[147] Second, the process of compelling fingerprints is also protected under the Fourth Amendment, even though fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[148] Warning that investigatory seizures not predicated on probable cause "would subject unlimited numbers of innocent persons to the harassment and ignominy incident to involuntary detention," the Court reiterates "nothing is more clear than that the Fourth Amendment was meant to prevent wholesale intrusions upon the personal security of our citizenry,

[146] 470 U.S. 811 (1985).
[147] 394 U.S. 724 (1969).
[148] *Id*. at 727.

whether these intrusions be termed "arrests" or "investigatory detentions."[149]

It is thus surprising that in *Hayes*, Justice White took an unexpected detour from the facts of that case and noted, unprompted, that *onsite* fingerprinting without probable cause or a warrant – a situation that was not before the court – would likely be constitutionally reasonable.[150] In his words, "[n]one of the foregoing implies that a brief detention in the field for the purpose of fingerprinting, *where there is only reasonable suspicion not amounting to probable cause*, is necessarily impermissible under the Fourth Amendment."[151] Thus, the Court seemed to be signaling to law enforcement that if only it would have brought a mobile fingerprinting kit to the suspect's house, they might have been able to gather the information they needed under the reasonable suspicion standard allowed in *Terry*.

In covertly instructing law enforcement about this procedural alternative to carting suspects down to the police station illegally, the Court reasoned that "fingerprinting, because it involves neither repeated harassment nor any of the probing into private life and thoughts that often marks interrogation and search, represents a much less serious intrusion upon personal security than other types of searches and detentions."[152] Certainly, MORIS fingerprinting fits well within the type of quick, accurate, onsite fingerprinting that Justice White contemplated. Justices Brennan and Marshall, in their concurrence, point out the dangers of the Majority's instruction, noting that it was at that time, "a police practice that, as far as we know, has never been attempted by the police in this or any other case." In fact, in reflecting on onsite fingerprinting in the absence of probable cause for arrest, they argue that it might fail under *Terry*, primarily because "an intrusion…would not be justifiable as necessary for the officer's protection."[153] The Justices also reflect on dignitary harms that onsite fingerprinting would cause detainees, noting that the practice, which would be "apparently undertaken in full view of any passerby," "would involve a singular intrusion

[149] *Id*. at 726.
[150] *Hayes v. Florida*, 470 U.S. 811, 816-17 (1985) ("There is thus support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the procedure is carried out with dispatch.").
[151] *Id*. at 816.
[152] *Id*. at 814.
[153] *Id*. at 819.

on the suspect's privacy…an intrusion that would not be justifiable (as was the pat-down in *Terry*) as necessary for the officer's protection."[154]

The Court's reflection in *Hayes* on the intrusiveness of fingerprinting is in some respects consistent with earlier rulings in *U.S. v. Schmerber*[155] and other cases[156] that the government is, under limited circumstances, permitted to conduct searches of the bodies of detainees; body searches including drawing blood,[157] placing a detainee's hands under an ultraviolet lamp,[158] taking fingernail scrapings,[159] removing hair from the head,[160] obtaining urine and saliva samples, and giving breathalyzer examinations.[161] Critically, however, these body searches were deemed permissibly conducted on *arrestees*. Certainly, they would not be permitted on *Terry* or *Hiibel* detainees in the context of protective searches or identity acquisition. In fact, the *Schmerber* Court reasoned that, "the interests in human dignity and privacy which the Fourth Amendment protects forbid…intrusions [beyond the body's surfaces] on the mere chance that desired evidence might be obtained. In the absence of a clear indication that in fact such evidence will be found, these fundamental human interests require law officers to suffer the risk that such evidence may disappear unless there is an immediate search."[162]

And although *Schmerber* is often cited for the proposition that warrantless blood draws are reasonable searches if supported by probable cause, the Court is emphatic that its holding is cabined to the narrow facts of that case, warning that "the integrity of an individual's person is a cherished value of our society. That we today [h]old that the Constitution does not forbid the States' minor intrusions into an individual's body under stringently limited conditions in no way indicates that it permits more substantial intrusions, or intrusions under other conditions."[163] This reasoning has, for the most part, held: In *Winston v. Lee*, the Court applied the *Schmerber* balancing test and held that society's interests in conducting surgery on an arrestee to remove a bullet to ascertain its

---

[154] *Id*.
[155] 384 U.S. 757 (1966).
[156] *See generally* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment*, §5.3(c).
[157] *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006).
[158] *Commonwealth v. DeWitt*, 314 A.2d 27 (1973).
[159] *Cupp v. Murphy*, 412 U.S. 291 (1973).
[160] *Coddington v. Evanko*, 112 Fed. Appx 935 (3d Cir. 2004).
[161] *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989).
[162] *Schmerber* at 770.
[163] Id. at 772.

origins did not outweigh the defendant's protected interests in keeping the state from forcing him to endure the administration of a general anesthetic, a two-hour surgery, and the risk of damage to muscle, nerve, and blood vessel tissue. [164]

As the best analogy for facial and iris scanning, fingerprinting is unsatisfying in its indeterminacy. Professor Laurence Tribe agrees, for example, that "an iris scan is almost certainly a 'search' within the meaning of the Fourth Amendment's protection against unreasonable searches and seizures" noting that like fingerprints, iris scans require a subject to be seized and will be used to "provide accurate non-public information about the person's true identity" while obtaining "information that is not as accurately obtainable by mere observation of what an individual chooses to expose to the world at large."[165] But does this mean that iris scanning practices should follow fingerprinting? And if so, what result? The two are not perfectly analogous: Iris scanning is arguably more invasive than fingerprinting, because it requires a subject to open his eyes and actively comply with officers' attempts to get high-quality scans. On the other hand, iris scans are used for now purely as an identification metric, and cannot be associated with past crimes in the way that fingerprints can. No person committing a crime, for example, leaves behind latent iris prints as evidence that may be used against him in court. Similarly, unlike facial scans, it is unlikely that irises prints will ever yield rich personal information about a person's social networking or political activities. Thus, while iris scans seem at first to be the most obvious candidates for enhanced protection from government acquisition and use, in important ways they present fewer practical privacy harms to the individuals they are associated with.

INFORMATION-RICH DATABASE PROTECTIONS AND HARMS

The *Hiibil* Justices were not unaware of the problems that compelling even a name—apart from other identity-linked information—may cause. In his *Hiibel* dissent, Justice Stevens noted "a name can provide the key to a great deal of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases. And that information, in turn, can be tremendously useful in a

[164] 470 U.S. 753 (1985).
[165] D. Parvaz, Mobile Biometrics to Hit U.S. Streets, at http://www.aljazeera.com/indepth/features/2011/07/20117258145965608.html (Aug. 2011).

criminal prosecution."[166] Justice Breyer agreed: "Indeed, as the majority points out, a name itself – even if it is not 'Killer Bill' or 'Rough 'em up Harry' – will sometimes provide the police with "a link in the chain of evidence needed to convict the individual of a separate offense." A name is, after all, but one conduit to other personally identifying information.

Indeed, although one value of a biometric system is to collect face, iris, and fingerprint data for identity acquisition or verification, law enforcement agencies may separately measure a system's value based on the amount of data it links to that name. As Sean Mullin of MORIS has said, "The database is the golden nugget of the whole thing."[167] Predicated on the earlier-developed Inmate Recognition and Identification System (IRIS), the MORIS system was designed to store fingerprint information used to identify and track prison inmates; IRIS is still used by over three hundred law enforcement agencies to track inmates as they move within and across facilities that comprise the massive systems of state and federal prisons. Alongside MORIS and IRIS, BI2 also makes and markets tools for the Child Project, Senior Safety Net, and the Sex Offender Registry & Identification System (SORIS).[168]

As MORIS's database and capabilities have expanded to encompass new law enforcement uses, multiple federal, state, and local law enforcement agencies have purchased the system. Funding that enables MORIS access originates with the Department of Justice, which earmarks money for a number of law enforcement related topics under an initiative known as Community Oriented Policing Services (COPS). The DOJ has distributed COPS money to the National Sheriffs' Association,[169] the Plymouth County Sheriff's office, and the Massachusetts Sheriff's Association,[170] enabling them to buy mobile biometric devices from BI2 Technologies.[171] And as more agencies use MORIS to collect information on individuals, the system's database grows exponentially.

---

[166] 542 U.S. 177, 196.
[167] Emily Steel and Julia Angwin, *Device Raises Fear of Facial Profiling*, THE WALL STREET JOURNAL at http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html?mod=WSJ_hp_LEFTTopStories&_nocache=1320619339678&user=welcome&mg=id-wsj (July, 2011).
[168] Brochure, Accenture Border Clearance Showcase, http://www.bi2technologies.com/products.
[169] BI2 Technologies, Pinal Sheriff's Office Sees Eye Scanners as the Future, http://www.bi2technologies.com/pinal-sheriffs-office-sees-eye-scanners-future (visited May 5, 2012).
[170] BI2 Technologies, Patriot Ledger: Brockton Police to Use Facial Recognition System , http://www.bi2technologies.com/patriot-ledger-brockton-police-use-facial-recognition-system (visited May 5, 2012).
[171] BI2 Technologies, http://www.bi2technologies.com/.

MORIS demonstrates that entities collecting information appear to have strong incentives to create databases that are not only large but also comprehensive in terms of the amount of information associated with a given entry in the system.

The over-collection and over-storage of data relative to the legitimate or initial purpose of a biometric system reduces transparency and increases the risk of function creep. Far more than revealing the suspect's identity, these databases appear primed to yield information about a suspect's entire criminal history. Technologically, an input of a facial photograph, an iris scan, or a fingerprint has the capacity to result in the return of all information that happens to be linked to the detainee's identity in the database that the device references. Chief William Conlon of the Brockton, Massachusetts Sheriff's department notes, "if [officers] encounter an individual who has warranted being identified…we'll be able to take their picture…and this will have facial recognition systems built into it that will go into a secure Internet connection…and it will come up with their picture from the previous event and *with their complete history*."[172] The database also appears to be accurate, if salesmanship is to be believed: Sean Mullin claims that "in the fourth quarter of 2010 [the MORIS family of identification software] performed 3.2 billion – that's *billion*, with a 'b' - successful cross matches with one false accept [a false positive match]."

Apart from collection and storage, there is the issue of distribution. Although B12 publicly claims to not own or sell the data within their database, it is not apparent how one would know if they did. Sean Mullin claims that B12 will not give private companies access to its iris database, but others speculate that recognition software could also be sold to private companies who might want to maintain a list of persons who ought to have access to their facilities and "black list" of persons to exclude. [173]

Moreover, improvement in mobile and wireless communications, as well as remote storage in cloud computing services, enabled biometric systems to move away from stationary deployments and into the field. These provide convenience, but also pose significant security risks. Each officer in the field is potentially holding a direct conduit to the largest biometric database the world has ever seen. Losing a device at a bar or club

[172] http://www.theblaze.com/stories/are-u-s-cops-preparing-widespread-use-of-facial-recognition-iphone/
[173] D. Parvaz, Mobile Biometrics to Hit U.S. Streets, at http://www.aljazeera.com/indepth/features/2011/07/20117258145965608.html (Aug. 2011).

will, without strict security controls, be a much greater problem than Apple losing track of its latest iPhone.

RECOMMENDATIONS

In the face of rapid technological advancements in mobile biometric technology, serious privacy harms accompanying its use, and the currently indeterminate landscape of substantive legal protections, I preliminarily propose best practices for law enforcement agencies seeking to develop procedures guiding the use of MORIS and similar devices. The goal of these recommendations is to promote certainty and allow officers to fulfill important and legitimate government interests of self and community security that the Supreme Court recognized in *Terry* and *Hiibel*, while also minimizing important dignitary, privacy, and security harms to individuals.

Best Practices

As a first principle, the use of mobile biometrics should be considered only if an officer first has the requisite reasonable suspicion needed to conduct an investigatory stop comporting with *Terry*. Under *Terry*, a protective stop may be conducted where a reasonably prudent officer is justified in believing that an individual presents a danger to his or others' safety and has committed, is committing, or is about to commit a crime, and where he can point to specific and articulable facts which, taken together with the rationale inferences from those facts, reasonably warrant that intrusion.[174]

If an officer subsequently determines, per *Hiibel*, that a request for identity is reasonably related to the scope of the circumstances that justified the stop, the officer may also request the detainee's name, and the individual should be allowed to able to provide oral or written identification of his choice. This ask-and-response comports with most narrowly with the provision of the Nevada statute upheld in *Hiibel*, and it both keeps the locus of control with the detainee and limits the scope of the inquiry to identity only. Normally, the officer's inquiry should end here.

Only if a person provides his name and the officer has a reasonable suspicion that the individual is not who he claims to be, and if that concern is reasonably related to the scope of the circumstances that justified the initial stop and the request for identity, and if the totality of the circumstances, amounts to probable cause for the detainee's arrest, should the inquiry proceed. Thus, reasonable suspicion about the veracity of the

[174] 392 U.S. 1, 30.

identification provided is itself a separate, third, prong in the analysis. "There is always the possibility that a police officer, lacking probable cause to obtain a search warrant, will use a traffic arrest as a pretext to conduct a search."[175]

Critically, however, probable cause should not be based on a mere misdemeanor offense, and should particularly not be predicated on doubts about identity itself. As Justice O'Connor and three other Justices noted in dissent in *Atwater v. City of Lago Vista*, [176] "Giving police officers constitutional carte blanche to effect an arrest wherever there is probable cause to believe a fine-only misdemeanor has been committed is irreconcilable with the Fourth Amendment's command that seizure's be reasonable." Instead, when there is probable cause to believe that a fine-only offense has been committed, the police officer should issue a citation unless the officer is 'able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonable warrant [the additional] intrusion of a custodial arrest.

If probable cause to arrest exists, the officer may use the MORIS device to conduct onsite identity checks that are the same, but do not exceed, standard administrative practice in his jurisdiction. "A policeman's on-the-scene assessment of probable cause provides legal justification for arresting a person suspected of crime, and for a brief period of detention, to take the administrative steps incident to arrest."[177] In many jurisdictions, this will allow officers to take a facial photograph of a detainee and also check his fingerprints. In fewer situations, an iris scan may also be permissible. But as a general principle, an officer should use only the more commonly accepted and less invasive components of MORIS: facial imaging or onsite fingerprinting. This is practical, in that it comports with standard station practice and does not potentially convert each use of the MORIS device into a constitutional challenge, and is more protective of a detainee's dignitary interests.

As a second principle, data minimization requirements should be put in place: these requirements should strictly limit the amount and type of information stored in the reference database, the amount and type of information that is returned to officers in the

[175] *United States v. Robinson*, 414 U.S. 218 (1973) (Justice Marshall, dissenting from the holding that in the case of a lawful custodial arrest a full search of the person is both an exception to the warrant requirement and a "reasonable" search under the Fourth Amendment).
[176] 532 US 318 (2001).
[177] *Gerstein v. Pugh*, 420 U.S. 103 (1975) (Justice Powell, writing for the majority).

field, and the amount and type of information that is uploaded to the database in the context of an onsite detainment. Data initially stored in the database and returned to officers in the field should be limited to criminal file information such as mug shots, fingerprints, and other identifiers, as well as outstanding warrants and parolee violations. Data that might be of interest to officers but that is derived from other sources, such as DMV records, civil employment files, or social networking sites, should not be in the database and should be subject to mandatory deletion if found.

Finally, as a minimal shore up against indiscriminate collection of biometric data, any legislative effort should follow the lead of New York State, which prohibits uploading that identifying information into an electronic database if the detainee is released without further legal action.[178] On the other hand, strict records should be kept about the demographic of the scanned individuals, in an effort to instill a culture of transparency and prepare for stricter auditing of detainments.

Fair Information Practice Principles (FIPPs)

When there is doubt about which action to take with respect to MORIS, I also recommend a Fair Information Practices approach to the collection, use, storage, and disclosure of biometric data coupled with reasonable controls on the initial field use of MORIS in the field. The Fair Information Practices provide specific, robust, and implementable privacy standards for law enforcement agencies engaged in the field use of mobile biometric devices. I consider here the articulation of FIPPs in the Department of Homeland Security's (DHS) 2008 Privacy Policy Guidance Memorandum.[179] Compared to prior versions of FIPPs that sometimes provided vague, incomplete, and

[178] *See* New York Criminal Procedure Law, Article 140, Arrest Without a Warrant, §140.50 Temporary questioning of persons in public places; search for weapons, available at http://ypdcrime.com/cpl/article140.htm#c140.50 ("In cities with a population of one million or more,[178] information that establishes the personal identity of an individual who has been stopped, questioned and/or frisked by a police officer or peace officer, such as the name, address or social security number of such person, shall not be recorded in a computerized or electronic database if that individual is released without further legal action; provided, however, that this subdivision shall not prohibit police officers or peace officers from including in a computerized or electronic database generic characteristics of an individual, such as race and gender, who has been stopped, questioned and/or frisked by a police officer or peace officer.").

[179] Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (accessed May 10, 2011).

generally weakened privacy protections,[180] the DHS framework is the U.S.-based framework that most closely follows strong international interpretations of FIPPs. These principles are as follows, modified only where needed to reflect current understanding of the needs of citizens, who have important dignitary, privacy, and security interests in their biometric information:

1. **Transparency**: Onsite law enforcement biometric data collection policies should be transparent and should provide meaningful, clear, full notice to the individual regarding the collection, use, dissemination, and maintenance of household energy usage data.

2. **Individual Participation**: Law enforcement agencies and peace officers should ask for individual consent for the collection, use, dissemination, and maintenance of biometric data. Law enforcement agencies should provide mechanisms for appropriate access, correction, and redress regarding entities' biometric data.

3. **Purpose Specification**: Law enforcement agencies and peace officers should specifically articulate the authority that permits the collection of onsite biometric data and specifically articulate the purpose or purposes for which that data is intended to be used.

4. **Data Minimization**: Law enforcement agencies and peace officers should only collect biometric data that is directly relevant and necessary to accomplish the specified purpose of detainee identification, and should only retain that data for as long as necessary to fulfill that specified purpose.

5. **Use Limitation**: Law enforcement agencies should use biometric data solely for the purpose specified in the notice given to detainees. Sharing biometric data outside the agency should be for a purpose compatible with the purpose for which it was collected and should comport with the Privacy Act of 1974.

6. **Data Quality and Integrity**: Law enforcement agencies should, to the extent practicable, ensure that biometric data is accurate. Any entity handling biometric data collected by officers, including data management service providers, should provide individuals with tools to correct mistakes or challenge information provided in profiles.

7. **Security**: Law enforcement agencies and any entity handling biometric data should protect the biometric data through appropriate security safeguards

[180] For an expansion of this critique, see CDT, Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable, http://www.cdt.org/privacy/20091105_ftc_priv_comments.pdf, at 6-7 (Nov. 6, 2009).

against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. **Accountability and Auditing**: Law enforcement agencies should be accountable for complying with these principles, providing training to all officrs and contractors who handle biometric data, and auditing the actual use of biometric data to demonstrate compliance with the principles and all applicable privacy protection requirements.

CONCLUSION

Although portable biometric identification technologies such as MORIS allow law enforcement officers to more efficiently serve the public interest by returning wanted felons and wayward parolees to prison, they also run the great risk of encouraging dragnet searches and profiling, imposing significant social costs for racial, ethnic, religious, and political minorities, and indeed all individuals who value anonymity and privacy as they go about their everyday lives. In the absence of strong Constitutional protections limiting law enforcement use of biometrics, particularly in criminal detainment contexts, new statutory direction is needed. Until Congress acts, however, state and local law enforcement agencies need procedural guidance so that officers may use MORIS and similar devices wisely and judiciously. It is important that agencies establish, and that officers observe, strict protocols limiting the use of MORIS to situations where probable cause to arrest exists, and to not step beyond the bounds of administrative identity acquisition already in place at police stations. Additionally, MORIS should not provide officers access to a master database of digital dossiers on innocent individuals culled from myriad non-criminal sources, the existence of which would harm the privacy of individuals and contravene the public interest.

APPENDIX

Figure 1. Images of MORIS Device.[181]

[181] http://modmyi.com/content/4916-police-beginning-adopt-iphone-based-facial-recognition-device.html; http://www.biometrics4you.com/news-items-july-2011.html

Table 2. Federal Biometric Initiatives (as of July 2012).[182]

AGENCY	INITIATIVE	BRIEF DESCRIPTION
DOD	Biometrics Identity Management Agency (BIMA)[183]	Formerly the Biometrics Task Force, BIMA is a permanent DOD organization that operates and maintains the DOD's biometric database. It is the executive manager of biometrics for the DOD,[184] and also helps coordinate inter-agency data sharing.[185]
DHS	REAL-ID[186]	REAL-ID establishes minimum standards for state-issued driver's licenses and identification cards, including requiring digital facial images.
	US-VISIT[187]	US-VISIT collects biometrics from all visitors entering the U.S.; it is used by ICE, the Coast Guard, DOD, DOJ, DOS, and USCIS.
	IDENT[188]	DHS-managed database of fingerprints, date of birth, nationality, and photographs submitted by a variety of collecting organizations.
	Secure Communities[189]	Secure Communities is a DHS-backed biometric information sharing partnership between ICE and the FBI that relies on local law enforcement biometric data collection for its implementation.
	Transportation Worker Identification Credential (TWIC)[190]	TWICs are tamper-resistant biometric credentials that allow unescorted personnel to access secure physical or computer areas of the national transportation system used by DHS and TSA.

[182] Biometrics.gov, http://www.biometrics.gov/ReferenceRoom/FederalPrograms.aspx (last visited April 30, 2011).
[183] Biometrics Identity Management Agency, http://www.biometrics.dod.mil/ (last visited April 30, 2011).
[184] Department of the Army, 2011 Posture Statement, *Biometrics: What is it?* (March 21, 2011), https://secureweb2.hqda.pentagon.mil/VDAS_ArmyPostureStatement/2011/information_papers/PostedDocument.asp?id=257.
[185] Biometrics Identity Management Agency, *Biometrics Identity Management Agency Overview*, http://www.biometrics.dod.mil/, ("As per DoD Directive 8521 01E, [BIMA] serves to: (1) Act as the DoD proponent for biometrics, (2) Lead in the development and implementation of biometrics technologies for Combatant Commands, Services and Agencies, (3) Deliver capabilities in order to contribute to the enhancement of the biometric community, (4) Increase Joint Service interoperability, and (5) Empower the warfighter by improving operational effectiveness on the battlefield.").
[186] U.S. Department of Homeland Security, *REAL ID Final Rule* (April 12, 2012), http://www.dhs.gov/files/laws/gc_1172765386179.shtm.
[187] U.S. Department of Homeland Security, *Government Agencies Using US-VISIT* (March 4, 2011), http://www.dhs.gov/files/programs/gc_1214422497220.shtm
[188] U.S. Department of Homeland Security, *Privacy Impact Assessment for the Interim Data Sharing Model (iDSM) for the Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability Project* (Sept. 1, 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_idsm.pdf.
[189] U.S. Department of Homeland Security, Immigration and Customs Enforcement (ICE), Secure Communities, http://www.ice.gov/secure_communities/ (last visited April 30, 2012).
[190] U.S. Department of Homeland Security, Transportation Security Administration, Program Information, *Transportation Worker Identification Credential* (TWIC), http://www.tsa.gov/what_we_do/layers/twic/program_info.shtm (last visited April 30, 2012).

AGENCY	INITIATIVE	BRIEF DESCRIPTION
	TSA's Registered Traveler[191]	Overseen by the TSA, Registered Traveler is a private-sector program designed to expedite commercial airfare security screening. This program was discontinued, though in the Spring of 2012 there were reports that the program could be making a comeback.[192]
	NEXUS[193]	NEXUS is a program for low-risk, pre-approved frequent travelers between the United States and Canada for air, sea, or land travel.
DOJ (FBI)	Biometric Center of Excellence (BCOE)[194]	BCOE was created by the FBI's Science and Technology Branch to be the FBI's "one-stop shop for biometrics collaboration and expertise," sponsoring applied research and prototyping, and providing training to law enforcement and "national security partners."
	Integrated Automated Fingerprint Identification System (IAFIS)[195]	Managed by the FBI, IAFIS is the world's largest biometric database. It contains a criminal file with fingerprints, mug shots, scars, tattoo photos, height, weight, hair color, eye color, and aliases of 70 million subjects submitted voluntarily by federal, state, and local law enforcement agencies. It also contains a civil file with fingerprints from 31 million federal government employees.
	Next Generation Identification System (NGI)[196]	NGI is an enhanced, scalable IAFIS + IDENT repository containing ten-print fingerprints and palm prints while enabling easier uploads of photos of scars, marks, and tattoos. It allows electronic submission of data and rapid searches of a Repository for Individuals of Special Concern (RISC).
	Combined Deoxyribonucleic Acid (DNA) Index System (CODIS) [197] & National DNA	CODIS is the FBI's automated DNA information processing system. It supports law enforcement efforts to identify DNA profiles developed from crime scene evidence where no suspect has been identified, by comparing records to DNA databases, including the NDIS, which contained over 10.6 million

[191] U.S. Department of Homeland Security, Transportation Security Administration, What We Do, http://www.tsa.gov/what_we_do/index.shtm.
[192] *See* Kip Hawley, *Why Airport Security is Broken—And How to Fix It*, WALL STREET JOURNAL, April 15, 2012 ("[T]he second that you create a population of travelers who are considered "trusted," that category of fliers moves to the top of al Qaeda's training list, whether they are old, young, white, Asian, military, civilian, male or female. The men who bombed the London Underground in July 2005 would all have been eligible for the Registered Traveler cards we were developing at the time.").
[193] U.S. Department of Homeland Security, U.S. Customs and Border Protection, *Nexus Fact Sheet*, available at http://www.cbp.gov/linkhandler/cgov/travel/trusted_traveler/nexus_prog/nexus_facts.ctt/nexus_facts.pdf (last visited April 30, 2012).
[194] FBI Biometric Center of Excellence, *Online Library* (Feb. 24, 2012), http://www.biometriccoe.gov/Resources/Online_Library.htm.
[195] FBI, *Integrated Automated Fingerprint Identification System*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited April 30, 2012).
[196] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi
[197] http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet

AGENCY	INITIATIVE	BRIEF DESCRIPTION
	Index System (NDIS)[198]	offender profiles (as of March 2012) contributed by federal, state, and local forensic laboratories.
	National Institute of Justice (NIJ)[199]	NIJ provides grant funding for a wide variety of biometrics research and development projects.
	Facial Identification Scientific Working Group (FISWG)[200] and the Magna Database[201]	Established by the BCOE in February 2009, the FISWG is a scientific working group focusing on facial identification. FISWG is primarily a research entity, though it also spearheads efforts to establish the Magna Database, a collection of 3D facial images.
DOS	U.S. Electronic Passport[202]	The Electronic Passport is a regular U.S. passport that includes a computer chip and digital photograph, enabling biometric comparison at international borders.
	Visa Application	The State Department engages in biometric identifier collections through its embassies as part of the visa application process. Although typical arrangements[203] appear to preclude the routine sharing of data with non-US governments, this is not always the case.[204]
NSF	Center for Identification Technology and Research (CITeR)[205]	CITeR is an NSF-funded Industry/University Cooperative Research Center focused on biometrics. Its research sites are West Virginia University, the University of Arizona, and Clarkson University.

[198] http://www.fbi.gov/about-us/lab/codis/ndis-statistics
[199] http://www.nij.gov/nij/topics/technology/biometrics/projects.htm
[200] http://www.fiswg.org/
[201] http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/research/2008_04_research01.htm
[202] http://travel.state.gov/passport/passport_2498.html
[203] http://sansalvador.usembassy.gov/faqs-biometrics.html ("Biometrics information collected during the visa application process will be maintained for official U.S. Government immigration and law enforcement purposes only, and will be treated in accordance with strict privacy laws. We do not routinely share information on individual visa applicants with any foreign government.")
[204] In Afghanistan, the United States Embassy provides training and money to enable Afghans to fingerprint and photograph all travelers — including but not limited to US citizens — who pass through Kabul International Airport. Data collected from the Afghan airport program is shared with the United States Embassy, the Afghan minister of the Interior, and the Afghan Intelligence Agency (the "National Directorate of Security") and is, according to the NY Times, part of an ongoing effort by the US government to fingerprint millions of Afghans. For more information, see http://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html.
[205] http://www.citer.wvu.edu/

Table 2. List of Leading Mobile Biometric Devices.[206]

PHYSICAL FORM OF THE MOBILE BIOMETRIC OR ACCESSORY	PRODUCT NAME	PRODUCT VENDOR
Integrated	Mobile Smart Sensors[207]	Authentec
Handheld	MORIS iCAM H100 3M Cogent BlueCheck II[208] MorphoIDent[209]	B1[2] Identity Solutions Iris ID 3M Cogent MorphoTrust
Suitcase	Guardian Jump Kit[210]	Cross Match
Kiosk	G3[211] PARmobile[212]	Speed Identity SmartMatic
Ruggedized	SEEK II[213] HIIDE 5[214] BioTRAC[215]	Cross Match MorphoTrust Northrop Grumman
Smart Phones and Tablets	mobileOne[216] iFMID 500[217]	Fulcrum Biometrics SIC
Mobile Applications and SDKs	URC Mobile[218]	Aware
Mobile Infrastructure	Biometric Services Platform (BioSP)[219] IdentityX[220]	Aware Daon
Biometrics in Motion	Iris on the Move[221]	SRI/Sarnoff

[206] *David Benini,* Getting Started - Mobile Biometrics, April 2012, http://www.planetbiometrics.com/creo_files/upload/article-files/120419_mobile_biometrics_-_getting_started.pdf at 9.
[207] http://www.authentec.com/a/Production/smartsensors_mobile.aspx
[208] http://www.cogentsystems.com/MobilesProdLine.asp
[209] http://www.morpho.com/identification/criminal-identification/handheld-terminals/morphoident/?lang=en
[210] http://www.crossmatch.com/guardian-r-jump-kit.php
[211] http://www.speed-identity.com/produkter/data-capture/speed-capture-g3.aspx
[212] http://www.smartmatic.com/solutions/id-management-solutions/view/article/next-generation-device-for-enrollment-of-people/#.T5d1zBxnMS5
[213] http://www.crossmatch.com/seekII.php
[214] http://www.morphotrust.com/pages/774-hiide-5
[215] http://www.is.northropgrumman.com/products/biotrac/index.html
[216] http://www.fulcrumbiometrics.com/FbF-mobileOne-p/200100.htm
[217] http://www.sic.ca/en/p_iPhone.php
[218] http://www.aware.com/biometrics/urc_mobile.html
[219] http://www.aware.com/biometrics/biosp_mobileenrollment.html
[220] http://identityx.com/products-overview-0
[221] http://www.sarnoff.com/products/iris-on-the-move

Table 3. Stop and Identify Statutes, by State.

STATE	STATUTE EXCERPT	CODE
Alabama	*"and may demand of him his **name, address and an explanation of his actions**"*	Ala. Code §15-5-30[222]
Arizona	*"A person detained under this section shall state the person's true full name, BUT SHALL NOT BE COMPELLED TO ANSWER ANY OTHER INQUIRY of a peace officer."*	Ari. Rev. Stat. Tit. 13, §2412[223]
Arkansas	*upon inquiry by a law enforcement officer, refuses to identify himself or herself and give **a reasonably credible account of his or her presence and purpose**;*	Ark. Code Ann. §5-71-213(a)(1)[224]
Colorado	*"...and may require him to give his **name and address**, **identification if available**, and an **explanation of his actions**. A peace officer shall not require any person who is stopped pursuant to this section to produce or divulge such person's social security number."*	Colo. Rev. Stat. §16-3-103(1)[225]
Delaware	*"and may demand the **person's name, address, business abroad and destination**."*	Del. Code Ann., Tit. 11, §§1902, 1321(6)[226]
Florida	*"requesting the person to **identify** himself or herself and **explain his or her presence and conduct**."*	Fla. Stat. §856.021(2)[227]
Georgia	*"requesting the person to **identify** himself and **explain his presence and conduct**."*	Ga. Code Ann. §16-11-36(b)[228]

[222] http://law.justia.com/codes/alabama/2006/14214/15-5-30.html
[223] http://www.azleg.gov/FormatDocument.asp?inDoc=/ars/13/02412.htm&Title=13&DocType=ARS
[224] http://law.justia.com/codes/arkansas/2010/title-5/subtitle-6/chapter-71/subchapter-2/5-71-213/
[225] http://www.state.co.us/gov_dir/leg_dir/olls/sl2001/sl_261.htm
[226] http://delcode.delaware.gov/title11/c019/sc01/index.shtml#P27_576
[227] http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0800-0899/0856/Sections/0856.021.html
[228] http://law.justia.com/codes/georgia/2006/16/16-11-36.html

Illinois	*"and may demand the **name and address** of the person and an **explanation of his actions**."*	Ill. Comp. Stat., ch. 725, §5/107-14[229]
Indiana	*" (1) **name, address, and date of birth**; or (2) driver's license, if in the person's possession;"*	Indiana Code §34-28-5-3.5[230]
Kansas	*"and may demand of the **name, address** of such suspect and **an explanation of such suspect's actions**."*	Kan. Stat. Ann. §22-2402(1)[231]
Louisiana		La. Code Crim. Proc. Ann., Art. 215.1(A)
Missouri	*"and demand of him his **name, address, business abroad and whither he is going**."*	Mo. Rev. Stat. §84.710(2) [Kansas City][232]
Montana	*"request the person's **name and present address and an explanation of the person's actions**"*	Mont. Code Ann. §46-5-401[233]
Nebraska	*"and may demand of him his **name, address and an explanation of his actions**."*	Neb. Rev. Stat. §29-829[234]
Nevada	*"Any person so detained shall **identify himself or herself**, BUT MAY NOT BE COMPELLED TO ANSWER ANY OTHER INQUIRY OF ANY PEACE OFFICER."*	Nev. Rev. Stat. §171.123[235]
New Hampshire		N.H. Rev. Stat. Ann. §594:2, §644:6
New Mexico	*"concealing one's true name or identity, or disguising oneself with intent to obstruct the due execution of the law or with intent to intimidate, hinder or interrupt any public officer or any other person in a legal performance of his*	N.M. Stat. Ann. §30-22-3 [concealing identity only][236]

[229] http://www.ilga.gov/legislation/ilcs/fulltext.asp?DocName=072500050K107-14
[230] http://www.in.gov/legislative/ic/2010/title34/ar28/ch5.html
[231] http://kansasstatutes.lesterama.org/Chapter_22/Article_24/22-2402.html
[232] http://www.moga.mo.gov/statutes/C000-099/0840000710.HTM
[233] http://data.opi.mt.gov/bills/mca/46/5/46-5-401.htm
[234] http://law.justia.com/codes/nebraska/2006/s29index/s2908029000.html
[235] http://law.justia.com/codes/nevada/2010/title14/chapter171/nrs171-123.html
[236] http://law.justia.com/codes/new-mexico/2011/chapter30/article22/section30-22-3/

	duty" is a petty misdemeanor	
New York	*"and may demand of him his **name, address and an explanation of his conduct**."*	N.Y. Crim. Proc. Law (CPL) §140.50[237]
North Dakota		N.D. Cent. Code §29-29-21
Ohio	*"NOTHING IN THIS SECTION REQUIRES A PERSON TO ANSWER ANY QUESTIONS BEYOND that **person's name, address, or date of birth**."*	Ohio Rev. Code §2921.29[238]
Rhode Island	*"and may demand of the person his or her **name, address, business abroad, and destination**"*	R.I. Gen. Laws §12-7-1[239]
Utah	*"and may demand his **name, address and an explanation of his actions**."*	Utah Code Ann. §77-7-15[240]
Vermont	*"The person may be detained only until the person **identifies himself or herself satisfactorily** to the officer."*[241]	Vt. Stat. Ann., Tit. 24, §1983[242] [Municipal and County]
Wisconsin	*"and may demand the **name and address of the person and an explanation of the person's conduct**."*	Wis. Stat. §968.24[243]

[237] http://ypdcrime.com/cpl/article140.htm#c140.50
[238] http://codes.ohio.gov/orc/2921.29
[239] http://www.lawserver.com/law/state/rhode-island/ri-laws/rhode_island_general_laws_12-7-1
[240] http://le.utah.gov/~code/TITLE77/htm/77_07_001500.htm
[241] Note that under *Hiibel*, this statute is probably unconstitutionally vague.
[242] http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=24&Chapter=059&Section=01983
[243] http://docs.legis.wisconsin.gov/statutes/statutes/968/24