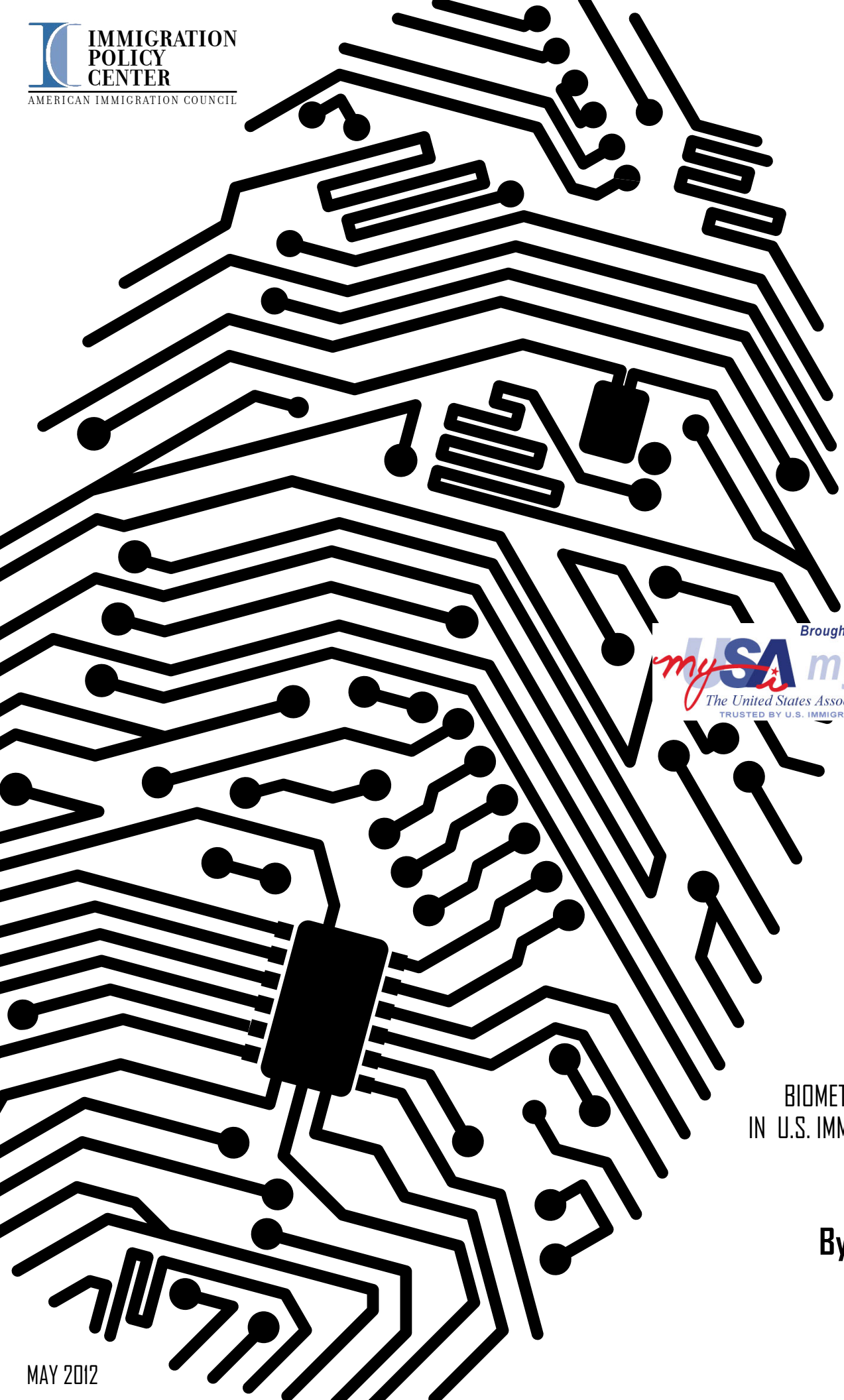
IMMIGRATION POLICY CENTER
AMERICAN IMMIGRATION COUNCIL



Brought to you by
myUSAi.org
The United States Association of Immigrants
TRUSTED BY U.S. IMMIGRANTS WORLDWIDE

FROM FINGER PRINTS TO DNA

BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND

By Jennifer Lynch

MAY 2012

SPECIAL REPORT

FROM FINGERPRINTS TO DNA:

BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND

BY JENNIFER LYNCH

MAY 2012

ABOUT SPECIAL REPORTS ON IMMIGRATION

The Immigration Policy Center's Special Reports are our most in-depth publication, providing detailed analyses of special topics in U.S. immigration policy.

ABOUT THE AUTHOR

Jennifer Lynch is a staff attorney with the Electronic Frontier Foundation and works on open government, transparency and privacy issues as part of EFF's FOIA Litigation for Accountable Government (FLAG) Project. In addition to government transparency, Jennifer has written and spoken frequently on government surveillance programs, intelligence community misconduct, and biometrics collection. Prior to joining EFF, Jennifer was the Clinical Teaching Fellow with the Samuelson Law, Technology & Public Policy Clinic at UC Berkeley School of Law. She has published academically on identity theft and phishing attacks (20 Berkeley Tech. L.J. 259) and sovereign immunity in civil rights cases (62 Fla. L. Rev. 203).

ABOUT THE ELECTRONIC FRONTIER FOUNDATION (EFF)

Blending the expertise of lawyers, policy analysts, activists, and technologists, the Electronic Frontier Foundation achieves significant victories on behalf of consumers and the general public. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 140,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public.

ABOUT THE IMMIGRATION POLICY CENTER

The Immigration Policy Center, established in 2003, is the policy arm of the American Immigration Council. IPC's mission is to shape a rational conversation on immigration and immigrant integration. Through its research and analysis, IPC provides policymakers, the media, and the general public with accurate information about the role of immigrants and immigration policy on U.S. society. IPC reports and materials are widely disseminated and relied upon by press and policymakers. IPC staff regularly serves as experts to leaders on Capitol Hill, opinion-makers, and the media. IPC is a non-partisan organization that neither supports nor opposes any political party or candidate for office. Visit our website at www.immigrationpolicy.org and our blog at www.immigrationimpact.com.

Table of Contents

Introduction

It's 10:30 in the morning in Los Angeles and Jose Sanchez,[1] an undocumented day laborer, stands on a corner with other men looking for work. Laborers like Jose[2] seek work with the tacit approval of the city,[3] but their status in the United States is tenuous. Suddenly, several Los Angeles Police Department (LAPD) officers ride up on bicycles. They pull out portable fingerprint scanners and tell all the men to line up and have their fingerprints scanned. The men, unsure of their rights but sure that they don't want to cause trouble, do so.

The fingerprint scanners the LAPD officers use are small and lightweight. They work with an officer's BlackBerry or smart phone and can run the day laborers' prints against more than four million prints currently on file in Los Angeles' local automated fingerprint identification system.[4] In less than two minutes of scanning each fingerprint, the officer knows whether any of the men has a criminal file or outstanding warrant. Also within that time, the City of Los Angeles has obtained a permanent record of each of the day laborers' biometric information, along with any biographical information or identification they provided to the officers.

The collection of biometrics—such as fingerprints, DNA, and face recognition-ready photographs—is becoming more and more a part of the society in which we live, no less so for immigrants within the United States. State and local law-enforcement agencies are quickly adopting mobile biometrics scanners like the fingerprint scanners in use by the LAPD,[5] though many of the newer scanners, like the "MORIS" (Mobile Offender Recognition and Information System),[6] are able to collect and identify much more than fingerprints—including iris prints and face images taken from several inches to several feet away.

Both the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are in the process of expanding their biometrics databases to collect much more information, including face prints and iris scans. As of January 2012, the FBI has been working with several states to collect face recognition-ready photographs of all suspects arrested and booked.[7] Once these federal biometrics systems are fully deployed, and once each of their approximately 100+ million records also includes photographs, it may become trivially easy to find and track people within the United States.

Undocumented people living within the United States, as well as immigrant communities more broadly, are facing these issues more immediately than the rest of society and are uniquely affected by the expansion of biometrics collection programs. Under DHS's Secure Communities program, states are required to share their fingerprint data—via the FBI—with DHS, thus subjecting undocumented and even documented[8] immigrants in the United States to heightened fears of deportation should they have any interaction with law enforcement. Further, under data-sharing agreements between the United States and other nations, refugees' biometric data may end up in the hands of the same repressive government they fled.[9] Should they ever be deported or repatriated, they could face heightened risks from discrimination or even ethnic cleansing within their former home countries.[10]

This paper addresses these issues. It discusses the state of biometrics in the United States today and its planned expansion in the future. It provides background information on biometrics and applicable laws and how biometrics and immigration issues intersect. It discusses concerns within the privacy advocacy community about biometrics, data sharing, and databases—and applies those concerns to immigration issues. Finally, it concludes with some proposals for change.

Background on Biometrics

What are Biometrics?

Biometrics are unique markers that identify or verify the identity of people using intrinsic physical or behavioral characteristics. Fingerprints are the most commonly known biometric, and they have been used regularly by criminal justice agencies to identify suspects for over a century.[11] Other biometrics include face prints (facial recognition-ready photographs), iris scans, palm prints, voice prints, wrist veins, hand geometry, a person's gait, DNA, and others. Biometrics fall into two general categories: physical and behavioral. Physical biometrics include unique biological and physiological features such as fingerprints, face prints, iris, and DNA. Behavioral biometrics are non-biological or non-physiological features such as distinctive and unique mannerisms and can include signature or keystroke patterns or even the path a person travels throughout her day.

Devices and Tools for Biometrics Collection

There are many ways to collect biometrics, though each falls into one of three general categories: 1) invasive, such as a blood sample, taken to collect a person's DNA; 2) minimally or non-invasive, such as a fingerprint or iris scan; or 3) collected without the subject's knowledge, such as photographs taken from a distance or DNA collected from discarded biological material. Each of these has different implications for privacy.

Minimally or non-invasive though known biometrics collection is most common. Most people living in the United States, including immigrants, have provided a biometric to a state or federal government agency through some minimally or non-invasive collection program. DHS collects approximately 300,000 fingerprints per day from non-U.S. citizens crossing the U.S. borders, and the State Department uses biometric identifiers in visas and other travel documents.[12] Anyone arrested and booked for a crime will be required to provide fingerprints, and many people who apply for a driver's license will provide face-recognition ready photographs.[13] And anyone who applies for employment with the federal government or for a sensitive position requiring a background check (such as working for law enforcement or with the elderly or young children) will be asked to supply a fingerprint.

Biometrics collection tools are getting smaller, more advanced, and less obtrusive, increasing their use for non-invasive though known, as well as unobtrusive, collection purposes. Increasingly, devices are portable, transmit data wirelessly, and are designed to allow collection, verification, and identification "in the field."[14] Many now include cameras, or like the MORIS (Mobile Offender Recognition and Information System),[15] work with devices in general use, such as the iPhone, to capture face-recognition ready photographs. This means law enforcement can carry biometrics collection tools with them in the field and can easily identify people on the fly.

Recent advances in camera and surveillance technology have improved the accuracy of biometrics capture and identification at a distance, making unobtrusive biometrics collection easier. These technologies, incorporated into private and public security cameras and other cameras already in use by police, are more capable of capturing the details and facial features necessary to support

facial recognition-based searches.[16] They can record high-quality photographs and video and store it for a long time.

Mobile biometrics scanners may connect to local, regional, statewide, or federal biometrics databases (or all four), or may connect to a database run by a private company under contract with the local law-enforcement agency.[18] Since September 2010, the FBI's mobile fingerprint scanners also communicate with and search against IDENT, the DHS biometric database, to facilitate data sharing under the Secure Communities program.[19]

Biometrics Collection and Storage

Biometrics can be stored in several ways, but in general, biometrics systems do not store the actual image of the biometric. Instead, they analyze the biometric to create a digital "template" (a mathematical representation) from it, which is made up of 1s and 0s. This template may then be stored in a database or on the scanning device itself to be used for matching and verification. The agency that collected the biometric may then chose to maintain it in its original form or discard it, retaining only the template.

Verification vs. Identification Systems

Biometrics are used for different purposes, but they are generally part of either a verification system or an identification system. The differences between these two types of systems can make a difference in how quickly the system operates and how accurate it is as the size of the database increases.

A **verification system** seeks to answer the question "Is this person who she says she is?" Under a verification system, an individual presents herself as a specific person ("I am Jennifer"). The system checks her biometric (such as an iris scan) against the biometric already in the database linked to that person's file (Jennifer's iris print) to try to find a match. Verification systems are generally described as a 1-to-1 matching system because the system tries to match the biometric presented by the individual against a specific biometric already on file. The E-Verify program, while not currently a biometrics program, is a verification-based system.[17] Because verification systems only need to compare the presented biometric to a biometric reference stored in the system, they can generate results more quickly and are more accurate than identification systems, even when the size of the database increases.

Identification systems are different from verification systems because an identification system seeks to identify an unknown person (or unknown biometric). The system tries to answer the questions "Who is this person?" or "Who generated this biometric?" and must check the biometric presented against all others already in the database. For this reason, identification systems are described as a 1-to-*n* matching system, where *n* is the total number of biometrics in the database. Forensic databases—where the government tries to identify a latent print or DNA discarded at a crime scene—often operate as identification systems.

Biometrics Databases and Data Sharing in the U.S. and Beyond

Biometrics Databases

Many different biometrics databases exist in the United States, but most are similar in that they combine a single biometric—generally a fingerprint—with a subject's biographical data, such as name, address, social security number, telephone number, e-mail address, booking and/or border crossing photos, gender, race, date of birth, immigration status, length of time in the United States, and unique identifying numbers (such as a driver's license number). The two largest biometrics databases in the world—and the two most likely to hold immigrants' data—are the FBI's Integrated Automated Fingerprint System (IAFIS) and DHS's Automated Biometric Identification System (IDENT), a part of its U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program.[20] Each database holds 100+ million records.

IAFIS's criminal file stores fingerprints taken from people arrested at the local, state, and federal level and also accepts latent prints taken from crime scenes. IAFIS's civil file stores fingerprints taken as part of a background check for many types of jobs, such as childcare workers, law-enforcement officers, lawyers, and federal employees. IAFIS includes over 71 million subjects in the criminal master file and more than 33 million civil fingerprints.[21] IAFIS supports over 18,000 law-enforcement agencies at the state, local, tribal, federal, and international level.

IDENT stores biometric and biographical data for individuals who interact with the various agencies under the DHS umbrella, including Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the U.S. Coast Guard, and others.[22] Through US-VISIT, DHS collects fingerprints from all international travelers to the United States who do not hold U.S. passports.[23] USCIS also collects fingerprints from citizenship applicants and all individuals seeking to study, live, or work in the United States through its two main programs, Refugees, Asylum and Parole Services (RAPS) and the Asylum Pre-Screening System (APSS).[24] And the State Department transmits fingerprints to IDENT from all visa applicants.[25] IDENT processes more than 300,000 "encounters" every day and has 130 million fingerprint records on file.[26]

In addition to the federal databases, each of the states has its own biometrics databases—generally a fingerprint database and a DNA database (described separately below)—and some regions like Los Angeles also have regional databases.[27] The prints entered into these databases are shared with the FBI, and under the Secure Communities program, FBI shares these prints with DHS to check a person's immigration status.

DNA Databases

DNA is unique to each individual and may become more widely used as an identifier in the near future—especially among immigrants—as the technology to collect and sequence DNA becomes faster and less expensive[28] and as collection devices become smaller and more capable of use in the field.[29]

Currently, the federal government and all 50 states collect DNA almost exclusively through the criminal justice system.[30] Since 2009, at least 21 states and the federal government have been collecting DNA from any adult arrested for (not just convicted of) a crime,[31] and 28 states collect DNA from juvenile offenders.[32] As a result of collecting DNA from arrestees, DNA collection in the United States has increased exponentially. In 2009 alone, nearly 1.7 million DNA samples were processed,[33] and as of December 2011, the National DNA Index or NDIS (the federal level of the FBI's Combined DNA Indexing System (CODIS)) contained over 10.7 million offender profiles and 423,000 forensic profiles.[34] Many of these belong to immigrants.

DHS may also begin collecting DNA in non-criminal contexts soon. USCIS, in partnership with the State Department, ran a pilot program in 2007 and 2008 to collect and test DNA from refugees in Africa who sought admission to the U.S.[35] Although there were many problems with the program, including that many individuals refused to consent to DNA testing,[36] the agencies seem poised to re-start the program in 2012 and possibly to expand it to other regions.[37] DHS is currently testing a portable "DNA analyzer," which it has said it plans to use in the field to determine kinship among refugees and asylum seekers, [38] and has discussed the program in a joint report to Congress on its plans for refugee admissions for 2012.[39]

DHS may also begin collecting DNA from others who interact with the agency. New rules promulgated by the Attorney General in 2009 require DHS to collect DNA from any non-United States person it detains.[40] DHS estimates this could affect up to 1 million people per year, including juveniles.[41] According to DHS, the DNA analyzer it is developing for the refugee and asylum context may in the future be used "to positively identify criminals [and] illegal immigrants."[42] Any expansion of DNA collection by DHS would have its greatest effect on immigrant populations.[43]

DNA databases are currently kept separate from fingerprint and other biometric databases, but similar databases exist at the local, state, and federal levels.[44] All 50 states, the federal government and the District of Columbia collect and share DNA records through the FBI's federal system called CODIS,[45] a "massive centrally-managed database linking DNA profiles culled from federal, state, and territorial DNA collection programs." [46] CODIS also includes profiles drawn from crime-scene evidence, unidentified remains, and genetic samples voluntarily provided by relatives of missing persons.[47]

Once a government agency has collected a genetic sample—either through a blood draw, a swab of the inner cheek, or by collecting discarded DNA—it is sent to a lab, which isolates the DNA from the sample and then processes it to obtain a "profile" from short fragments of repeated nucleotide sequences (short tandem repeats or "STRs") within inactive genes (sometimes called "junk DNA"[48]). These DNA profiles are entered as data into DNA databases like CODIS, along with an anonymized "Specimen Identification Number"[49] that links the profile to an individual.

DNA presents privacy issues different from those involved in other biometrics collection. If a DNA sample is collected through a blood draw or a swab of the inner cheek, its collection is inherently more invasive than purely external biometrics collection such as a fingerprint or photograph. Further, depending on the quality of the sample collected, it can contain information about a person's entire genetic make-up, including gender, familial relationships, and other hereditary information, race, health, disease history and predisposition to disease, and perhaps even sexual orientation.[50]

Although a DNA profile does not currently yield the more sensitive information about a person that is contained in a DNA sample, it presents its own privacy issues. Once DNA is in CODIS, "it will remain there permanently and can be continually accessed and searched . . . by police at any level of government . . . without any consent, suspicion, or warrant."[51] The DNA sample, which is not destroyed after the profile is created, presents additional issues. The sample contains significant information about a person—much more than any other biometric currently collected—and at least one circuit court has recognized, "[t]he concerns about DNA samples being used beyond identification purposes are real and legitimate."[52]

Interoperability and Data Sharing

Before September 11, 2001, the federal government had many policies and practices in place to silo data and information within each agency. Since that time the government has enacted several measures that allow—and in many cases require—information sharing within and among federal intelligence and federal, state, and local law-enforcement agencies.[53] For example, currently the FBI, DHS, and Department of Defense's biometrics databases are interoperable, which means the systems can easily share and exchange data.[54] This has allowed information sharing between FBI and DHS under ICE's Secure Communities program.[55]

Similarly, DHS is now sharing its data on asylum applicants more broadly with non-DHS agencies, per federal regulation 8 CFR §208.6(a). According to a June 30, 2011, Privacy Impact Assessment, DHS now shares the entire Refugees, Asylum and Parole Services (RAPS) database with the National Counter Terrorism Center (NCTC), a division of the Office of the Director of National Intelligence, under a Memorandum of Understanding (MOU).[56]

And states are sharing biometric data with the federal government as well. In addition to sharing criminal fingerprint and DNA profile data with the FBI, states are sharing fingerprints indirectly with DHS through Secure Communities. And some states are also sharing DMV face-recognition data with the FBI on an ad hoc basis.[57]

Corporate and Foreign Biometric Data Collection and Sharing

The collection of biometric and biographic data is not limited to federal, state, and local governments. Private companies and foreign governments also collect extensive amounts of biometric data. Because many private and foreign biometrics systems are linked to or accessible by government systems and employees, and because immigrant data are caught up in these systems, they could have a significant impact on privacy and immigrant communities.

One of the best-known private biometrics databases is maintained by Facebook. Facebook's face recognition service allows users to find and tag their friends,[58] and due to the high number of photos uploaded to and tagged on Facebook,[59] the service has seen dramatic increases in accuracy over the last several years. Facebook currently has over 845 million monthly active users, and requires each of those users to sign up under their real names.[60] Facebook then makes its users' names and primary photos public by default.[61] The government regularly mines this data to verify citizenship applications,[62] for evidence in criminal cases,[63] and to look for threats to U.S. safety and

security.[70] It is likely the government will try to find a way to take advantage of Facebook's face recognition service for each of these purposes soon.

The federal government does not appear to have formal data-sharing arrangements with private companies that collect biometrics, but it does have such arrangements with foreign governments. The FBI's Criminal Justice Information Service (CJIS) division has information-sharing relationships with 77 countries.[71] Also, ICE and the FBI have a draft agreement allowing them to share information on deportees with the countries to which they are deported, and DHS has entered into agreements with foreign governments to provide such information on deportees upon repatriation.[72] This kind of biometrics sharing could prove disastrous for repatriated refugees or immigrants from countries with a history of ethnic cleansing.

Concerns about Biometrics, Databases, and Data Sharing

The extensive collection and sharing of biometric data at the local, national, and international level should raise significant concerns among immigrant communities and Americans more broadly. Data sharing can be good for solving crimes across borders or jurisdictions, but can also perpetuate inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible.

Information and data fluidity within and among federal, state, and local agencies often makes it difficult to determine where information came from originally. This is problematic, as it increases the probability that data inaccuracies—such as notoriously inaccurate and out-of-date immigration records[73]—will be perpetuated throughout all systems. This has happened with the Secure Communities program, where approximately 3,600 United States citizens have been caught up in the program due to incorrect immigration records.[74]

Secure Communities Exemplifies the Problems

ICE's Secure Communities program shows how a program with a stated purpose to remove "those who pose a danger to national security or public safety"[64] can easily devolve. Under Secure Communities, when state and local law enforcement collect fingerprints from arrestees and run them against the FBI's IAFIS database, IAFIS automatically shares that data with DHS's US-VISIT program and IDENT database to check the arrestee's immigration status. If US-VISIT finds either an indication that the person lacks lawful status or finds a "no match," ICE will issue a detainer on the person until the agency can take him into custody. As such, through data-sharing, ICE is able to conscript state and local law enforcement to enforce immigration laws.

According to government statistics, there have been approximately 155,800 deportations since Secure Communities began in 2008.[65] In fiscal year 2011, out of the 79,797 people who were deported under S-Comm, 20,568 were never convicted of any crime, while 23,214 were only convicted of Level 3 offenses—crimes punishable by less than one year, including driving without a license.[66] In California alone, there have been more than 60,640 deportations, since Secure Communities started in 2008,[67] and these have included victims and relatives of victims of domestic abuse and people arrested under mistaken identity.[68] ICE does not wait until a person has been convicted of a crime to begin deportation proceedings. According to many law-enforcement agencies, Secure Communities has had negative effects on community policing efforts.[69]

FBI's Next Generation Identification

The FBI's Next Generation Identification (NGI) database represents the most robust effort to introduce and streamline multimodal biometrics collection. FBI has stated it needs "to collect as much biometric data as possible . . . and to make this information accessible to all levels of law enforcement, including International agencies." Accordingly, it has been working "aggressively to build biometric databases that are comprehensive and international in scope."[75]

Once NGI is complete, it will include iris scans, palm prints,[76] and voice data, in addition to fingerprints. However, the biggest and perhaps most controversial change will be the addition of face-recognition ready photographs, which the FBI has already started collecting through a pilot program with four states.[77] Unlike a traditional mug shot, NGI photos may be taken from any angle and may include close-ups of scars, marks and tattoos. They may come from public and private sources, including from private security cameras, and may or may not be linked to a specific person's record (for example, NGI will include crowd photos in which many subjects may not be identified). NGI will allow law enforcement, correctional facilities, and criminal justice agencies at the local, state, federal, and international level to submit and access photos, and will allow them to submit photos in bulk. It may also, in the future, allow law-enforcement agencies to identify subjects in publicly available photographs, such as those posted on Facebook or elsewhere on the Internet.[78]

DHS also appears poised to expand IDENT to include additional biometrics, which would further increase data sharing through Secure Communities.[79] Expanding these systems to incorporate multiple biometrics and allowing these systems to share information with little control over access to the data will make identifying and tracking people in the United States easier than ever.

Data sharing can also mean that data collected for non-criminal purposes, such as immigration-related records, is combined with and being used for criminal or national-security purposes with little to no standards, oversight, or transparency. When some of this data comes from sources such as local fusion centers and private security guards in the form of Suspicious Activity Reports (SARs),[80] it can perpetuate racially motivated targeting of immigrant communities.[81]

Advanced Biometrics Systems Exacerbate These Problems

Traditionally, biometrics databases such as IAFIS and IDENT have collected only one biometric at a time.[82] However, the government has argued these "unimodal" systems are limited and has been pushing to develop "multimodal" systems that collect and combine two or more biometrics (for example, photographs and fingerprints). The government argues that collecting multiple biometrics from each subject will make identification systems more accurate.[83]

Additional Concerns with Advanced Biometrics

The addition of advanced biometrics like facial-recognition-ready photographs or DNA capable of being collected without a person's knowledge to traditional biographic databases exacerbates the problems inherent in current biometrics systems and leads to new problems. For example, the addition of crowd and security camera photographs means that anyone could end up in the database—even if they're not involved in a crime—by just happening to be in the wrong place at the wrong time, by fitting a stereotype that some in society have decided is a threat, or by, for example, engaging in suspect activities in areas rife with cameras.[84] And as Americans have learned from experience with immigration databases, Suspicious Activity Reports, terrorist watchlists, and the Automated Targeting

System,[85] if any of the data in the system is inaccurate and propagated throughout several other systems, it can be extremely difficult to correct.[86]

Standardization of biometrics data causes additional concerns. Once data are standardized, they become much easier to use as linking identifiers, not just in interactions with the government but also across disparate databases and throughout society. For example, Social Security numbers were created to serve one purpose—to track wages for Social Security benefits—but are now used to identify a person for credit and background checks, insurance, to obtain food stamps and student loans, and for many other private and government purposes.[87] If biometrics become standardized, they could replace social security numbers, and the next time someone applies for insurance, sees her doctor, or fills out an apartment rental application, she could be asked for her thumbprint or iris scan. This is problematic if records are ever compromised because biometric information, unlike a unique identifying number such as a Social Security Number, cannot be changed. And the many recent security breaches show that the government can never fully protect against these kinds of data losses.[88] Data standardization also increases the ability of government or private companies to locate and track a given person throughout their lives.

Extensive data retention times can lead to additional problems. Biometric records stored in IDENT are retained for 75 years or until the statute of limitations for all criminal violations has expired.[89] Civil fingerprints stored in IAFIS are not destroyed until "the individual reaches 75 years of age," and criminal fingerprints not destroyed until "the individual reaches 99 years of age."[90] This is problematic because data that may be less identifying today could become more identifiable in the future as technology improves. For example, although faces recorded in a photograph of a large protest march might not be identifiable now, technologists are currently working on ways to make those faces identifiable in the future. Similarly, the "junk DNA" contained in CODIS DNA profiles could be found in the future to contain information about a person's genetic predisposition for disease or behavior and would therefore reveal much more information than just who the person is.

Technical Problems Specific to Facial Recognition

Technical issues specific to some biometrics such as facial recognition make their use worrisome for immigrant communities. For example, facial recognition's accuracy is strongly dependent on consistent lighting conditions and angles of view.[91] It also may be less accurate with certain ethnicities and with large age discrepancies (for example, if a person is compared against a photo taken of himself when he was ten years younger). These issues can lead to a high rate of false positives—when, for example, the system falsely identifies someone as the perpetrator of a crime or as having overstayed their visa. In a 2009 New York University report on facial recognition, the researchers noted that facial recognition "performs rather poorly in more complex attempts to identify individuals who do not voluntarily self-identify . . . Specifically, the "face in the crowd" scenario, in which a face is picked out from a crowd in an uncontrolled environment."[92] The researchers concluded the challenges in controlling face imaging conditions and the lack of variation in faces over large populations of people[93] make it unlikely that an accurate face recognition system will become an "operational reality for the foreseeable future."[94]

Some have also suggested the false-positive risk could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities.[95] This can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the

defendant to show he is *not* who the system identifies him to be. In light of this, German Federal Data Protection Commissioner Peter Schaar has noted that false positives in facial recognition systems pose a large problem for democratic societies. "[I]n the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[96]

Legal Protections for Privacy in Biometric Data

The Fourth Amendment's protection against unreasonable searches and seizures presents the baseline protection for biometrics collection in the United States. Yet while the Fourth Amendment applies to everyone in the United States regardless of citizenship or immigration status, there are significant exceptions to its protections that are relevant, both for biometrics and for immigrants. For example, although the Supreme Court has noted that fingerprints likely have some Fourth Amendment protection,[97] the Court has declined to define the boundaries of that protection and suggested in dicta that because "[f]ingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search[,]" perhaps that protection is limited.[98]

Courts have found greater protection in the collection of biological material such as blood or urine that "can reveal a host of private medical facts about an [individual]," finding the collection "intrudes upon expectations of privacy that society has long recognized as reasonable."[99] However, courts have cabined that protection in certain "special needs" circumstances, such as to ensure safety in transportation workers,[100] or where courts have found a person's rights are diminished due to a prior felony conviction[101] or having been arrested.[102]

Courts have also found that the government's interest in protecting United States borders justifies a broad exception to the Fourth Amendment's warrant requirement.[103] According to case law, the government may stop and search individuals and their possessions at the borders without suspicion and may search a person's body based only on reasonable suspicion (rather than probable cause).[104] This exception to the Fourth Amendment's warrant requirement has broad implications for immigrants in the United States because so much data on travelers is collected at the borders.

However, this case law may not map well to biometrics collection that doesn't involve a detention. In each of the cases discussed above, the legal analysis hinged in large part on the detention required to obtain the biometric data or on a "a meaningful interference with [one's] possessory interest in his bodily fluids."[105] Because biometrics such as DNA and face prints can be obtained without an initial detention and may be obtained without the subject's knowledge while the subject is in a public place, these protections may not apply to cases involving biometrics collected *after* a detention and *with* a suspect's knowledge. Several cases have held that suspects have no legitimate expectation of privacy in biological material obtained under similar circumstances,[106] or in discarded or abandoned material (such as garbage) or evidence in public view.[107]

However, a case recently decided by the Supreme Court, *United States v. Jones*,[108] could provide some insight into how courts could apply the Fourth Amendment to technologies such as biometrics that enable advanced surveillance and intrusive data collection, often in public without

an initial detention or seizure. In *Jones* the Court addressed whether a GPS device planted on a car without a warrant and used to track a suspect's movements constantly for 28 days violated the Fourth Amendment. Nine justices held that it did. For five of those justices, a person's expectation of privacy in not having his movements tracked constantly—even in public—was an important factor in determining the outcome of the case.[109] The fact that several members of the Court were willing to reexamine the reasonable expectation of privacy test[110] in light of newly intrusive technology could prove important for future legal challenges to biometrics collection.

Proposals for Change

The over-collection of biometrics has become a real concern, especially for immigrants and immigrant communities in the United States, but there are still opportunities—both technological and legal—to prevent the problem from getting worse.

Given the uncertainty of Fourth Amendment jurisprudence in the context of biometrics and the fact that biometrics capabilities are currently undergoing "dramatic technological change,"[111] legislative action could be a good solution to curb the over-collection and over-use of biometrics in society today and in the future. If so, the federal government's response to two seminal wiretapping cases in the late 60s could be used as a model.[112] In the wake of *Katz v. United States*[113] and *New York v. Berger*,[114] the federal government enacted the Wiretap Act, 18 U. S. C. §§2510–2522, which laid out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, and a notice provision.[115] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been governed primarily by statute rather than case law.

If legislation or regulations are proposed in the biometrics context, the following principles should be considered to protect privacy and security. These principles are based in part on key provisions of the Wiretap Act and in part on the Fair Information Practice Principles (FIPPs), an internationally recognized set of privacy protecting principles.[116]

- **Limit the Collection of Biometrics**—The collection of biometrics should be limited to the minimum necessary to achieve the government's stated purpose. For example, collecting more than one biometric from a given person is unnecessary in many situations. Similarly, the government's acquisition of biometrics from sources other than the individual to populate a database should be limited. For example, the government should not obtain biometrics en masse to populate its criminal databases from sources such as state DMV records, where the biometric was originally acquired for a non-criminal purpose, or from crowd photos.

- **Define Clear Rules on the Legal Process Required for Collection**—Each type of biometric should be subject to clear rules on when it may be collected and which specific legal process—such as a court order or a warrant—is required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should be defined to govern when law enforcement or similar agencies may collect "abandoned" biometrics such as DNA, or biometrics revealed to the public, such as a face print.

- **Limit the Amount and Type of Data Stored**—For biometrics such as DNA that can reveal much more information about a person than his or her identity, rules should be set to limit the amount of data stored. For example, if DNA must be collected for identification purposes, the sample should be destroyed immediately after the profile is extracted and entered into the database. Similarly, techniques should be employed to avoid over-collection of biometrics such as face prints (such as from security cameras or crowd photos) by, for example, scrubbing the images of faces that are not central to an investigation.

- **Limit the Combination of More than One Biometric in a Single Database**—Different biometric data sources should be stored in separate databases. If biometrics need to be combined, that should happen on an ephemeral basis for a particular investigation. Similarly, biometric data should not be stored together with non-biometric contextual data that would increase the scope of a privacy invasion or the harm that would result if a data breach occurred. For example, combining facial recognition technology from public cameras with license plate information increases the potential for tracking and surveillance. This should be avoided or limited to specific individual investigations.

- **Limit Retention**—Retention periods should be defined by statute and should be limited to no longer than necessary to achieve the goals of the program. Data that is deemed to be "safe" from a privacy perspective today could become highly identifying tomorrow. For example, a data set that includes crowd images could become much more identifying as technology improves. Similarly, data that was separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her biometric from the system if, for example, the person has been acquitted or is no longer under investigation.[117]

- **Define Clear Rules for Use and Sharing**—Biometrics collected for one purpose should not be used for another purpose. For example, biometrics such as fingerprints collected for use in a criminal context should not automatically be used or shared with an agency to identify a person in an immigration context. Similarly, photos taken in a non-criminal context, such as for a driver's license, should not be shared with law enforcement without proper legal process.

- **Enact Robust Security Procedures to Avoid Data Compromise**—Because biometrics are immutable, data compromise is especially problematic. Using traditional security procedures, such as basic access controls that require strong passwords and exclude unauthorized users, as well as encrypting data transmitted throughout the system, is paramount. However security procedures specific to biometrics should also be enacted to protect the data. For example, data should be anonymized or stored separate from personal biographical information. Strategies should also be employed at the outset to counter data compromise after the fact and to prevent digital copies of biometrics. For example, biometric encryption[118] or "hashing" protocols that introduce controllable distortions into the biometric before matching can reduce the risk of data compromise. The distortion parameters can easily be changed to make it technically difficult to recover the original privacy-sensitive data from the distorted data, should the data ever be compromised.[119]

- **Mandate Notice Procedures**—Because of the real risk that people's biometrics will be collected without their knowledge, biometrics rules should define clear notice requirements to alert people to the fact that their biometrics have been collected. The notice provision should also make clear how long the biometric will be stored and how to request its removal from the database.

- **Define and Standardize Audit Trails and Accountability Throughout the System**—All database transactions, including biometric input, access to and searches of the system, data transmission, etc. should be logged and recorded in a way that assures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

- **Ensure Independent Oversight**—every entity that collects or uses biometrics must be subject to meaningful oversight from an independent entity, and individuals whose biometrics are compromised should have a strong and meaningful private right of action.

Conclusion

Biometrics collection and its accompanying privacy concerns are not going away. Given this, it is imperative that government act now to limit unnecessary biometrics collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before biometric collection; and define clear rules for data sharing at all levels. This is important not just for immigrants and immigrant communities, but also for democratic society as a whole.

ENDNOTES

[1] "Jose Sanchez" is a pseudonym. His experience is representative of experiences reported by undocumented day laborers currently seeking work in Los Angeles.

[2] Day laborers' immigration status varies. A 1999 study of day laborers in Southern California found that it was "difficult to estimate the percentage of undocumented immigrants among the day labor population" and that, at the time, "close to 40 percent of day laborers interviewed in this survey believe[d] they [were] eligible to obtain legal resident documents." See Abel Valenzuela, Jr., *Day Laborers in Southern California: Preliminary Findings from the Day Labor Survey* (Center for the Study of Urban Poverty, Institute for Social Science Research, 1999).

[3] See City of Los Angeles Day Laborer Program, http://www.ci.la.ca.us/cdd/emp_empday.html (last visited Jan. 6, 2012). Day laborers are also supported by non-profits including the Coalition for Humane Immigrant Rights of Los Angeles, www.chirla.org, and the National Day Laborer Organizing Network, http://www.ndlon.org.

[4] See Cogent Systems, "BlueCheck mobile identification systems for Los Angeles police" *Pro Security Zone* (Sept. 23, 2008), http://www.prosecurityzone.com/News/Biometrics/Fingerprint_recognition/Bluecheck_mobile_identification_systems_for_los_angeles_police_5099.asp (last visited Jan. 6, 2012).

[5] LAPD acquired 500 mobile fingerprint scanners in 2005. According to a *Police Chief* article, as of 2009, most of the law-enforcement agencies patrolling the 4,000 square miles of Los Angeles County, including one federal agency, the Los Angeles Sheriff's Department, "the California Highway Patrol, and over 40 municipal police agencies, including the LAPD and the Long Beach Police Department," are using mobile fingerprinting devices. See Leo M. Norton, "Who Goes There? Mobile Fingerprint Readers in Los Angeles County," *The Police Chief* (June 2009), available at http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1824&issue_id=62009.

[6] See, e.g., Emily Steele, "How a New Police Tool for Face Recognition Works," Wall St. J. Digits Blog (July 13, 2011), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/.
[7] Aliya Sternstein, "FBI to launch nationwide facial recognition service," NextGov.com (Oct. 7, 2011), http://www.nextgov.com/nextgov/ng_20111007_6100.php.
[8] See, e.g., Aarti Kohli, et al., *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, 4 (Oct. 2011), available at http://www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf (noting that "1.6% of cases we analyzed were U.S. citizens and all were apprehended by ICE" and that, by extrapolating the numbers, this meant that "3,600 US citizens have been apprehended by ICE from the inception of the program through April 2011").
[9] Achraf Farraj, Note, "Refugees and the Biometric Future: The Impact of Biometrics on Refugees and Asylum Seekers," 42, *Colum. Hum. Rts. L. Rev.* 891, 920-921 (2011).
[10] Ibid.
[11] See, e.g., Biometrics Identity Mgmt. Agency, "Biometrics History Timeline," http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx (last visited Jan. 6, 2012) (discussing early uses of biometrics and the establishment of the Department of Justice's National Bureau of Criminal Identification as a centralized fingerprint repository in 1905).
[12] See Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act), Pub. L. No. 107-173, § 303(b)(1), 116 Stat. 543, 553 (2002); Tien-Li Loke Walsh & Bernard P. Wolfsdorf, "Consular Processing—The New Electronic Era," 1768 PLI/Corp 177 (2009), available at http://www.wolfsdorf.com/articles/Article%20-%20Consular%20Processing%20in%202010%20-%20The%20New%20Electronic%20Era%208%2010.pdf (describing State Department and DHS programs incorporating biometric identifiers). The United States is not alone in requiring biometrics for identification—by 2007, approximately 40 countries, including Germany, Australia, South Africa, and Poland have incorporated biometrics into their travel documents. See Farraj, supra note 9 at 910.
[13] See Thomas Frank, "Four states adopt 'no-smiles' policy for driver's licenses," *USA Today*, May 25, 2009, http://www.usatoday.com/news/nation/2009-05-25-licenses_N.htm (noting that, at the time of the article, 31 states had already started using some form of facial recognition with their DMV photos, generally to stop fraud and identity theft).
[14] For example, some scanners can capture fingerprints and facial portraits and allow an officer to swipe a driver's license to get biographical information. See "MobileID Solution," Cogent Systems, http://www.cogentsystems.com/downloads/MobileID_WhitePaper-COGT_sm.pdf (last visited Jan. 6, 2012); see also "Cogent Systems Receives Orders for its BlueCheck™ Portable Bluetooth Fingerprint Scanner from the Los Angeles Police Department" (Jul. 17, 2007), http://www.findbiometrics.com/articles/i/4589/. Other systems can capture and store thousands of records of forensic-quality fingerprints, latent fingerprints, iris images, photos, and textual data and transmit that data wirelessly (Ibid).
[15] See, e.g., Emily Steele, "How a New Police Tool for Face Recognition Works," Wall Street Journal Digits Blog (July 13, 2011) http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/. Face recognition will likely be added soon to body-mounted video cameras worn by police. See, e.g., Erica Goode, Video, "A New Tool for the Police, Poses New Legal Issues, Too," *N.Y. Times* (Oct. 11, 2011), available at https://www.nytimes.com/2011/10/12/us/police-using-body-mounted-video-cameras.html (discussing cameras in current use); Wasseem Al-Obaydy & Harin Sellahewa, "On using high-definition body worn cameras for face recognition from a distance," *Biometrics and ID Management* (Lecture Notes in Computer Science 6583, 194-205 (March 2011), available at http://www.springerlink.com/content/p225k89r38381m55. Also available at http://www.ioptec.com/images/stories/pdf/uni.pdf.
[16] For a discussion of specific technologies, see Jennifer Lynch, "FBI Ramps Up Next Generation ID Roll-Out—Will You End Up in the Database?" Electronic Frontier Foundation (Oct. 19, 2011), https://www.eff.org/deeplinks/2011/10/fbi-ramps-its-next-generation-identification-roll-out-winter-will-your-image-end.
[17] See U.S. Citizenship and Immigrations Services, "E-Verify," http://www.dhs.gov/e-verify. The e-Verify system checks the data a prospective employee provides to the employer with the data already resident in the database. It also allows an employer to visually check the photograph on the federal identification document presented by the prospective employee against the photograph in the system to determine if the photographs are the same.
[18] For example, the LAPD system checks prints against a regional database called the "Los Angeles County Regional Identification System" (LACRIS). See http://la-sheriff.org/divisions/tsdiv/record_id/ri_ovrview.html#lacris.
[19] See IIU Report, Biometric Interoperability (Nov. 24, 2010), Bates Numbered FBI-SC-FPL-00458-461, available at http://uncoverthetruth.org/wp-content/uploads/11-10-11-Released-Documents-Index.pdf. Notes in these documents assert that for the FBI Mobile users, the "additional data from IDENT can be used as 'traction' by FBI Agents during criminal investigations."
[20] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.
[21] See http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Apr. 26, 2012).

[22] See "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," DHS (July 31, 2006), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. IDENT was originally developed for the legacy Immigration and Naturalization Services in 1994.

[23] Customs and Border Protection (CBP) feeds biometrics data into IDENT while also maintaining its own database, called TECS, which includes personally identifiable information on and biometrics obtained from travelers crossing the border into the United States. See DHS, "Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing" ("TECS PIA"), DHS/CBP/PIA-009(a), (Dec. 22, 2010), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

[24] DHS, "Privacy Impact Assessment for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System" (Nov. 24, 2009), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_rapsapss.pdf. USCIS also maintains its own database of "biometric images," including a digital photograph and signature, both of which appear on an applicant's naturalization certificates. See DHS, "Privacy Impact Assessment Update for the Computer Linked Application Information Management System, DHS/USCIS/PIA-015(a), (Aug. 31, 2011), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_claimsupdate.pdf (describing capturing of "digitized biometric images" through the Benefits Biometric Support System (BBSS)).

[25] *See* DHS, "Government Agencies Using US-VISIT," http://www.dhs.gov/files/programs/gc_1214422497220.shtm.

[26] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[27] See, supra n. 18.

[28] A 2010 report prepared for the Department of Defense noted that by 2013, the cost of sequencing the entire human genome should drop to $100. See JASON (The MITRE Corporation), *The $100 Genome: Implications for the DoD*, at 11 (Dec. 15, 2010).

[29] Currently, DNA processing is experiencing such backlogs that using DNA to identify someone is not feasible on a large scale. See Mark Nelson, *Making Sense of DNA Backlogs, 2010 — Myths vs. Reality*, 1, 8, National Institute of Justice, U.S. Department of Justice (Feb. 2011), available at http://www.ncjrs.gov/pdffiles1/nij/232197.pdf (noting the "year-end backlog of offender samples has increased steadily, from 657,166 in 2007, to 793,852 in 2008, to 952,393 in 2009" and that some laboratories do not consider a case backlogged until the DNA has not been analyzed for 90 days).

[30] See http://www.fbi.gov/about-us/lab/codis.

[31] See National Conference of State Legislatures, *State Laws on DNA Data Banks—Qualifying Offenses, Others Who Must Provide Sample* (Feb. 25, 2010), http://www.ncsl.org/issues-research/civil-and-criminal-justice/state-laws-on-dna-data-banks.aspx. See also 42 U.S.C. 14135a (federal DNA Fingerprint Act of 2005) and the Attorney General's rules on DNA collection: "DNA-Sample Collection Under the DNA Fingerprint Act of 2005 and the Adam Walsh Child Protection and Safety Act of 2006," 28 CFR Part 28 (Jan. 9, 2009), available at http://www.uscis.gov/ilink/docView/FR/HTML/FR/0-0-0-1/0-0-0-145991/0-0-0-165820/0-0-0-169744.html.

[32] Council for Responsible Genetics, "Introduction and Summary of Findings," *National DNA Databases*, http://www.councilforresponsiblegenetics.org/dnadata/exec.html.

[33] U.S. Department of Justice, National Institute of Justice, "Making Sense of DNA Backlogs, 2010—Myths vs. Reality" at p. 8 (Feb. 2011), available at http://www.ncjrs.gov/pdffiles1/nij/232197.pdf.

[34] See FBI, *CODIS—NDIS Statistics*, http://www.fbi.gov/about-us/lab/codis/ndis-statistics (last visited Apr. 26, 2011). State DNA databases are expanding as well. For example, as of January 2012, California had 1.9 million offender profiles. See Jan Bashinski DNA Laboratory, "Monthly Statistics," available at http://ag.ca.gov/bfs/pdf/Monthly.pdf (last visited Apr. 26, 2012).

[35] See Jill Esbenshade, *An Assessment of DNA Testing for African Refugees*, Immigration Policy Center (Oct. 2010), available at http://www.immigrationpolicy.org/special-reports/assessment-dna-testing-african-refugees.

[36] Ibid. See also U.S. State Dept., *Fact Sheet: Fraud in the Refugee Family Reunification (Priority Three) Program* (Feb. 3, 2009), available at http://www.state.gov/j/prm/releases/factsheets/2009/181066.htm.

[37] See *Proposed Refugee Admissions for Fiscal Year 2012—Report to the Congress*, U.S. State Dept., DHS, U.S. Dept. Health & Human Svcs., 12 (Oct. 17, 2011), available at www.state.gov/documents/organization/181378.pdf (noting that the State Department and USCIS were still reviewing the program as of the end of FY 2011 and that once the agencies restarted the program it would likely include "a DNA relationship testing component for certain claimed biological relationships.").

[38] William Matthews, "New portable DNA screener to debut this summer," *NextGov.com* (Feb. 24, 2011), http://www.nextgov.com/nextgov/ng_20110224_1299.php. The Department of Defense is also testing rapid DNA analyzers. See Press Release, "IntegenX Proves Rapid Human DNA Identification Utility at DOD Exercise" (June 20, 2011), available at http://integenx.com/june202011.

[39] *Proposed Refugee Admissions for Fiscal Year 2012—Report to the Congress*, U.S. State Dept., DHS, U.S. Dept. Health & Human Svcs., 12.

[40] See 28 C.F.R.§ 28.12(b) (directing "any agency of the United States that arrests or detains individuals or supervises individuals facing charges shall collect DNA samples . . . from non-United States persons who are detained under the authority of the United States").

[41] See Jennifer Lynch, EFF "DHS Considers Collecting DNA From Kids; DEA and US Marshals Already Do," https://www.eff.org/deeplinks/2012/04/dhs-considers-collecting-dna-kids-dea-and-us-marshals-already-do.
[42] Ibid.
[43] DHS may detain "non-United States persons" for purely civil rather than criminal purposes, so this could mean hundreds of thousands of people who have never interacted with the criminal justice system could end up having their DNA in a database. See, e.g., Julia Preston, "Immigrants' DNA to flood U.S. database," *International Herald Tribune* (Feb. 5, 2007), https://www.nytimes.com/2007/02/05/world/americas/05iht-dna.4481568.html (quoting Justice Department officials as saying "the goal . . . is to make DNA sampling as routine as fingerprinting for anyone detained by federal agents" and noting that in 2006, "federal customs, Border Patrol and immigration agents detained more than 1.2 million immigrants.").
[44] These are known as a LDIS (Local DNA Index System), SDIS (State DNA Index System), or NDIS (National DNA Index System). See "Levels of the Database," *DNA Initiative*, http://www.dna.gov/dna-databases/levels (last visited Mar. 15, 2012).
[45] FBI, "Combined DNA Index System (CODIS)," http://www.fbi.gov/about-us/lab/codis.
[46] See *United States v. Kincade*, 379 F.3d 813, 819 (9th Cir. Cal. 2004).
[47] Ibid.
[48] Ibid. at 818.
[49] See FBI, *Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System*, http://www.fbi.gov/about-us/lab/codis/codis-and-ndis-fact-sheet (last visited Mar. 15, 2012).
[50] See, e.g., *United States v. Kriesel*, 508 F.3d 941, 948 (9th Cir. 2007)(quoting *Kincade*, 379 F.3d at 842 n.3 (9th Cir. 2004)(en banc)(Gould, J., concurring))(noting that "DNA stores and reveals massive amounts of personal, private data about that individual," including "the person's health, their propensity for particular disease, their race and gender characteristics, and perhaps even their propensity for certain conduct"); *Kincade*, 379 F.3d at 850 (Reinhardt, J., dissenting) (quoting Harold J. Kent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 Tex. L. Rev. 49, 95-96 (1995).
[51] Ibid. See also Generations Ahead, *Report: Forensic DNA Database Expansion: Growing Racial Inequalities, Eroding Civil Liberties and Diminishing Returns*, available at http://www.generations-ahead.org/files-for-download/success-stories/GenerationsAhead_ForensicDNADatabaseExpansion2011_(1).pdf.
[52] *Kriesel*, 508 F.3d at 948.
[53] This was achieved through provisions in the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), several Executive Orders (Exec. Order No. 13356, 69 C.F.R. 53599 (2004), Exec. Order No. 13355, 69 C.F.R. 53593 (2004), Exec. Order No. 13354, 69 C.F.R. 53589 (2004), Exec. Order No. 13311, 68 C.F.R. 45149 (2003)), and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).
[54] The National Institute for Standards and Technology (NIST), along with other standards setting bodies, has developed standards for the exchange of biometric data. See National Institute for Standards and Technology, ANSI/NIST-ITL 1-2011, *American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* (2011), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136.
[55] For more on Secure Communities, see Michele Waslin, *The Secure Communities Program: Unanswered Questions and Continuing Concerns*, Immigration Policy Center (Nov. 2011).
[56] Dep't of Homeland Sec., *Privacy Impact Assessment Update for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System,* DHS/USCIS/PIA-027(a) (June 30, 2011), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_raps_update_nctc.pdf. DHS has been sharing asylum data with the FBI since October 8, 2001, per an MOU signed by the agencies on that date. See USCIS Asylum Division, *Fact Sheet on Confidentiality*, 6 (June 15, 2005), available at http://www.usa-federal-forms.com/uscis-index-html/uscis-fact-sheet-on-confidentiality-uscis-5413.html.
[57] The FBI has already worked with North Carolina to track criminals using the state's DMV records. Mike Baker, "FBI uses facial-recognition technology on DMV photos," *USA Today* (Oct. 13, 2009), http://www.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm.
[58] Facebook promotes its facial recognition service as an efficient way to tag photos and makes it difficult to turn off this feature. See, e.g., Eva Galperin, "How to Disable Facebook's Facial Recognition Feature," EFF (June 9, 2011) www.eff.org/deeplinks/2011/06/how-disable-facebooks-facial-recognition-feature.
[59] Face.com, the company that provides the technology to enable Facebook's facial recognition and automatic tagging system, states that it has indexed 31 billion face images. See Yaniv Taigman and Lior Wolf, "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition," Face.com, http://face.com/research/faceR2011b.html (last visited Mar. 15, 2012).
[60] See Emil Protalinski, "Facebook has over 845 million users," *ZDNet* (Feb. 1, 2012), http://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332; Facebook "Statement of Rights and Responsibilities" (April 26, 2011), https://www.facebook.com/legal/terms.
[61] Facebook, "Control Over Your Profile," http://www.facebook.com/about/privacy/your-info-on-fb#controlprofile (last visited April 27, 2012).

[62] See Jennifer Lynch, "Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend,'" Electronic Frontier Foundation (Oct. 12, 2010), https://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and (describing how USCIS agents "friend" applicants for citizenship on social networking sites in order to monitor them).
[63] The Department of Justice Criminal Division regularly requests all photos in which a user is tagged in its warrants for Facebook data. See Jennifer Lynch, "DOJ Wants to Know Who's Rejecting Your Friend Requests," Electronic Frontier Foundation (Jan. 24, 2012), https://www.eff.org/deeplinks/2012/01/doj-wants-know-who%E2%80%99s-rejecting-your-friend-requests.
[64] According to ICE, this includes "aliens engaged in or suspected of terrorism or espionage, or who otherwise pose a danger to national security[.]" See ICE, "Secure Communities: Advancing ICE's Priorities," http://www.ice.gov/secure_communities/.
[65] *Secure Communities: Monthly Statistics through November 30, 2011: IDENT/IAFIS Interoperability*, ICE, 2, ICE.gov, available at http://www.ice.gov/doclib/foia/sc-stats/nationwide_interoperability_stats-fy2012-to-date.pdf.
[66] As the Immigration Policy Center noted in its Special Report on the Secure Communities program, DHS statistics show that in FY 2010, nearly 31,000 "convicted criminal aliens" were removed with criminal traffic violations listed as their crime, and "criminal traffic violations" was the third most common category of criminal conviction, after convictions for dangerous drug offenses and criminal immigration violations. See Michele Waslin, *The Secure Communities Program: Unanswered Questions and Continuing Concerns*, Immigration Policy Center (Nov. 2011), available at http://www.immigrationpolicy.org/sites/default/files/docs/Secure_Communities_112911_updated.pdf. In March 2011, ICE suggested its agents and officers should exercise discretion when dealing with minor traffic offenses. See Memorandum, "Civil Immigration Enforcement: Priorities for the Apprehension, Detention, and Removal of Aliens" (Mar. 2, 2011), available at www.ice.gov/doclib/news/releases/2011/110302washingtondc.pdf. Nevertheless, despite ICE's stated changed priorities, the practices on the ground do not appear to have changed significantly. See, e.g., Edgar Aguilasocho, et al., *MISPLACED PRIORITIES: The Failure of Secure Communities in Los Angeles County*, Immigrant Rights Clinic, UC Irvine School of Law, 2 (Jan. 2012), available at http://law.uci.edu/pdf/MisplacedPriorities_aguilasocho-rodwin-ashar.pdf.
[67] *Secure Communities: Monthly Statistics through November 30, 2011: IDENT/IAFIS Interoperability*, 4, ICE, http://www.ice.gov/doclib/foia/sc-stats/nationwide_interoperability_stats-fy2012-to-date.pdf.
[68] See Lee Romney & Paloma Esquivel, "Noncriminals swept up in federal deportation program," *L.A. Times* (Apr. 25, 2011), available at http://articles.latimes.com/2011/apr/25/local/la-me-secure-communities-20110425; Paloma Esquivel, "Immigrant advocates urge ending Secure Communities program" *L.A. Times* (Aug. 18, 2011), available at http://articles.latimes.com/2011/aug/18/local/la-me-0817-secure-communities-20110817.
[69] Ibid.
[70] Jennifer Lynch, "New FOIA Documents Reveal DHS Social Media Monitoring During Obama Inauguration," EFF.org (Oct. 13, 2010), https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media; Jennifer Lynch, "Government Uses Social Networking Sites for More than Investigations," EFF.org (Aug. 16, 2010), https://www.eff.org/deeplinks/2010/08/government-monitors-much-more-social-networks. The FBI is currently looking for software to make its mining of social-media data more efficient and to allow it to map communities of interest. See Jim Giles, "FBI releases plans to monitor social networks," *New Scientist* (Jan. 25, 2012), http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html.
[71] See Fed. Bureau of Investigation/Criminal Justice Info. Servs. (CJIS) Advisory Policy Board Identification Services Subcommittee, *Issue Paper: Biometrics Information Sharing Update* (Spring 2011), Bates No. SC-FBI-FPL-1088-89, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1081.pdf") (noting these relationships are "in the form of both informal (ad hoc, verbal) agreements and formal agreements (Memoranda of Agreement, Memoranda of Understanding, Letter of Cooperation)."). This contrasts with FBI's statements on its website, noting that since 2002, the Global Initiatives Unit CJIS has "developed relationships with more than 50 countries and has received over 450,000 biometric records that have been added to IAFIS." See "Biometric Sharing Initiative: Making the World Safer," FBI (Jan. 14, 2011) available at http://www.fbi.gov/news/stories/2011/june/biometrics_061411/biometrics_061411.
[72] Ibid. at SC-FBI-FPL-1089; DHS, "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," 8 (July 31, 2006) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf.
[73] See generally Joan Friedland, National Immigration Law Center, *INS Data: The Track Record*, available at www.nilc.org/document.html?id=233 (citing multiple Government Accountability Office and Inspector General reports on inaccuracies in immigration records). These problems persist. See generally, e.g, U.S. Government Accountability Office (GAO), *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Jan. 18, 2011), available at http://www.gao.gov/products/GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors).
[74] See, e.g., Aarti Kohli, et al. *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, at p.4, Chief Justice Earl Warren Institute on Law and Social Policy, UC Berkeley School of Law (Oct. 2011), available at www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf.

[75] See *Statement: Interoperability Initiatives Unit* (December 2010), Bates No. SC-FBI-FPL-1043, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1043.pdf")

[76] According to the FBI, the Bureau received 1.2 million palm prints in fiscal year 2011 at a daily average of 3,170 prints. See IAFIS Fact Sheet, available at http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts. The daily average in fiscal year 2012 so far is 4,838. Ibid.

[77] These states include Michigan, Washington, Florida, and North Carolina. See Aliya Sternstein, "FBI to Launch Nationwide Facial Recognition Service," Nextgov.com (Oct. 7, 2011), available at http://www.nextgov.com/nextgov/ng_20111007_6100.php.

[78] See, e.g., Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, 5, FBI available at http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf (noting another goal of NGI is to "Identify[ ] subjects in public datasets"). Further, although the FBI's 2008 Privacy Impact Assessment (PIA) stated that the NGI/IAFIS photo database does not collect information from "commercial data aggregators," the PIA acknowledged this information could be collected and added to the database by other NGI users like state and local law-enforcement agencies. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, FBI (June 9, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[79] See "Accenture Awarded Biometric Identity System Contract from U.S. Department of Homeland Security," *Wall Street Journal Market Watch* (Dec. 21, 2011), at http://www.marketwatch.com/story/accenture-awarded-biometric-identity-system-contract-from-us-department-of-homeland-security-2011-12-21; Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[80] See, e.g., G.W. Schulz & Andrew Becker, "Finding Meaning In Suspicious Activity Reports," *NPR* (Sept. 7, 2011), http://www.npr.org/2011/09/07/140237086/finding-meaning-in-suspicious-activity-reports; ACLU, *More About Suspicious Activity Reporting* (June 29, 2010), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting.

[81] See, e.g., Robert Smith, "Julia Shearson tells how a weekend trip to Canada became 5-year fight for rights," *The Plain Dealer* (June 4, 2011), available at http://blog.cleveland.com/metro/2011/06/julia_shearson_tells_how_a_wee.html (describing how Executive Director of the Cleveland Council on American-Islamic Relations (CAIR) ended up on an FBI terrorist watchlist and her struggle to correct inaccuracies in her government files).

[82] Press Release, *DHS Begins Collecting 10 Fingerprints From International Visitors At Washington Dulles International Airport*, DHS (Dec. 10, 2007), available at http://www.dhs.gov/xnews/releases/pr_1197300742984.shtm.

[83] *Next Generation Identification*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited April 27, 2012).

[84] For example, in Lower Manhattan, where the Occupy protests started, the New York Police Department has installed as many as 3,000 security cameras. See Noah Shachtman, "NYC Is Getting a New High-Tech Defense Perimeter. Let's Hope It Works," *Wired* (Apr. 21, 2008), http://www.wired.com/politics/security/magazine/16-05/ff_manhattansecurity.

[85] The Automated Targeting System assigns everyone who crosses United States borders, whether citizen or non-citizen, a computer-generated 'risk assessment' score. Data collected by ATS is "stored for 15 years, even for individuals who have not been flagged as a threat or potential risk." See Shana Dines, "Interim Report on the Automated Targeting System: Documents Released through EFF's FOIA Efforts," EFF.org (Summer 2009), https://www.eff.org/pages/interim-report-autom. Under ATS, individuals have no way to access information about their "risk assessment" scores or to correct any false information about them. See "Lawsuit Demands Answers About Government's Secret 'Risk Assessment' Scores," EFF (Dec. 19, 2006), https://www.eff.org/press/archives/2006/12/19.

[86] See n. 81, infra.

[87] See "Legal requirements to provide your SSN," Social Security Online, http://ssa-custhelp.ssa.gov/app/answers/detail/a_id/78/~/legal-requirements-to-provide-your-ssn.

[88] See, e.g., David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *N.Y. Times* (May 23, 2006), available at https://www.nytimes.com/2006/05/23/washington/23identity.html.

[89] DHS, *Privacy Impact Assessment (PIA) for the Automated Biometric Identification System (IDENT)* (Jul. 31, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf.

[90] FBI, *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purpose—Channeling* (May 5, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

[91] Face recognition technologies perform well when all the photographs are taken with similar lighting and shot from a frontal perspective (like a mug shot). However, with different lighting, shadows, different backgrounds, different poses or expressions, or as a person ages, the error rates are significant. See, e.g., P. Jonathon Phillips, et al., "An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem," *National Institute of Standards & Testing* (Dec. 2011), available at www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs that are "difficult to match." Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real

terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, 190 (2003).

[92] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April 2009), available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[93] In layman's terms, this means that because so many people within a given population look alike, the probability that any facial recognition system will regularly misidentify people becomes much higher as the data set (the population of people you are checking against) gets larger.

[94] Ibid. at 47.

[95] Ibid. at 45-46.

[96] Ibid. at 37.

[97] *Davis v. Mississippi*, 394 U.S. 721, 723-24 (1969) (excluding from evidence fingerprints obtained during an illegal detention). See also *Hayes v. Florida*, 470 U.S. 811, 817 (1985) (noting in dicta that the Fourth Amendment would permit a "brief detention in the field for the purpose of fingerprinting . . . if there is reasonable suspicion that the suspect has committed a criminal act, [and] if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime[.]"); *Cupp v. Murphy*, 412 U.S. 291, 295 (1973) (implying that a person subjected to fingerprinting had less of a Fourth Amendment interest than someone subjected to a search of their fingernails because the former was a search of publicly-exposed physical characteristics). Other cases have relied on the Fifth Amendment to limit the amount of information a police officer can seek from a person stopped. See, e.g., *Hiibel v. Sixth Jud. Dist. Ct. of Nev.*, 542 U.S. 177 (2004). However, the testimonial nature of the information requested (such as an address or other private details about a person's background) has been a key distinction in this line of cases. Because biometrics such as fingerprints are considered "physical evidence," they likely are not considered "testimonial," and the Fifth Amendment's protections against incrimination may not apply. See, e.g., *Schmerber v. California*, 384 U.S. 757, 765 (1966) (holding that neither the extraction of blood nor its chemical analysis for the purpose of a blood-alcohol test is testimonial); but see *Schmerber*, 384 U.S. at 764 (recognizing that some "physical evidence" such as the results of a lie detector test, are designed to elicit responses and are therefore "essentially testimonial").

[98] *Schmerber*, 384 U.S. at 728.

[99] S*kinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 617 (1989). See also *Schmerber*, 384 U. S. at 767-68 (recognizing that "compelled intrusio[n] into the body for blood to be analyzed for alcohol content" must be deemed a Fourth Amendment search).

[100] *Skinner*, 489 U.S. at 620. See also *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646 (1995) (holding that collecting urine from high school students participating in extracurricular activities to detect and prevent drug use was a special need).

[101] *United States v. Kriesel*, 508 F.3d 941 (9th Cir. 2007) (DNA collection from all convicted felons is reasonable after amendment to 42 U.S.C. §§14135-14135e); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004) (same for felons convicted of certain enumerated crimes).

[102] See, e.g., *United States. v. Mitchell*, 652 F.3d 387 (3d Cir. 2011) (finding that DNA collection from arrestees does not violate the Fourth Amendment because arrestees have a diminished expectation of privacy in their identities, and DNA collection from arrestees serves important law enforcement interests); but see *King v. State*, No. 68 (September Term 2011), 2012 Md. LEXIS 211, *3-4 (Md. Ct. App. Apr. 24, 2012) (holding suspicionless DNA collection from an arrestee is an unconstitutional search).

[103] See *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004); see also e.g., *Carroll v. United States*, 267 U.S. 132, 154 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in.").

[104] See, e.g., *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985) (rectal examination of traveler was reasonable under circumstances of case).

[105] *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 618 n.4 (1989).

[106] See Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 Calif. L. Rev. 721, 736 n.63 and accompanying text (2007) (citing cases).

[107] See, e.g., *California v. Greenwood*, 486 U.S. 35 (1988) (no reasonable expectation of privacy in garbage left on the street); *California v. Ciraolo*, 476 U.S. 207 (1986) (no expectation of privacy in backyard that can be viewed from a plane flying above); Elizabeth Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 863-64 (2006) (distinguishing cases where courts have found a "meaningful interference with an individual's possessory interests" from cases where "suspects 'knowingly expose' items to public view").

[108] 565 U.S. ____ (2012).

[109] *Id.* (slip op. at 2-3) (Sotomayor, J. concurring); *Id.* (slip op. at 9–12) (Alito, J., concurring).

[110] See *Katz v. United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring).

[111] *Jones*, 565 U.S. ____, (slip op. at 13) (Alito, J., concurring).

[112] In Justice Alito's concurrence in the *Jones* case discussed above, he specifically referenced post-*Katz* wiretap laws and called out for legislative action, noting "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id*. (slip op. at 11, 13) (Alito, J., concurring).
[113] 389 U.S. 347 (1967).
[114] 388 U.S. 41 (1967). *Berger* was unique in that it struck down a state wiretapping law as facially unconstitutional. In striking down the law, the Court laid out specific principles that would make a future wiretapping statute constitutional under the Fourth Amendment.
[115] See, e.g., Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 851-52 (2004).
[116] See Privacy Act of 1974, 5 U.S.C. § 552a (2010). See also Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. The full version of the FIPPs as used by DHS includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. See Hugo Teufel III, Chief Privacy Officer, DHS, Mem. No. 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. See also *Fair Information Practice Principles*, Fed.Trade Commission, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).
[117] For example, in *S. and Marper v. United Kingdom*, the European Court of Human Rights held that retaining cellular samples and DNA and fingerprint profiles of people acquitted or people who have had their charges dropped violated Article 8 of the European Convention on Human Rights. *S. and Marper. v. United Kingdom*, App. Nos. 30562/04 and 30566/04, 48 Eur. H.R. Rep. 50, 77, 86 (2009).
[118] See, e.g., Information and Privacy Commissioner, Ontario, Canada, *Privacy-Protective Facial Recognition: Biometric Encryption—Proof of Concept* (Nov. 2010), available at www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf.
[119] See, e.g., Center for Unified Biometrics and Sensors, "Cancellable Biometrics," SUNY Buffalo, http://www.cubs.buffalo.edu/cancellable.shtml (last visited Mar. 15, 2012).