IMMIGRATION POLICY CENTER
AMERICAN IMMIGRATION COUNCIL

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:

PROBLEMS WITH 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.

EXECUTIVE SUMMARY

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, especially for immigrants. As of January 2012, the Federal Bureau of Investigation (FBI) has been working with several states to collect face recognition-ready photographs of all suspects arrested and booked. The Department of Homeland Security (DHS) collects approximately 300,000 fingerprints per day from non-U.S. citizens crossing U.S. borders. State and local law-enforcement agencies are quickly adopting and expanding several biometrics databases to collect much more information, including face prints, iris scans, and even DNA records. Undocumented people living within the United States, as well as immigrant communities more broadly, are more immediately and uniquely affected by the expansion of biometrics collection programs than the rest of society.

The rapid expansion of programs that collect, store, and share biometric data has raised important concerns over privacy and data accuracy for citizens and non-citizens alike. This report summarizes these programs and their implications, and outlines best practices for developing effective and responsible biometrics programs in the future.

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. 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.

There are many ways to collect biometrics, though each falls into one of three general categories:

- **invasive biometrics**, i.e. blood sample, taken to collect a person's DNA.
- **minimally or non-invasive biometrics**, i.e. a fingerprint or iris scan.
- **biometrics collected without the subject's knowledge**, i.e. photographs taken from a distance or DNA collected from discarded biological material.

Once biometric information is collected, it can be used for one of two purposes—verification or identification:

1. A verification system seeks to answer the question "Is this person who she says she is?" The system checks her biometric (such as an iris scan) against the biometric already in the database linked to that person's file (her iris print) to try to find a match.
2. 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.

Where is Biometric Information Stored and Who Can Access It?

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. 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. This has allowed information sharing between FBI and DHS under Immigration and Customs Enforcement's Secure Communities program.

Private companies and foreign governments also collect extensive amounts of biometric data. The FBI's Criminal Justice Information Service (CJIS) division has information-sharing relationships with 77 countries. One of the best-known private biometrics databases is maintained by Facebook, whose face-recognition service allows users to find and tag their friends. The government regularly mines this data to verify citizenship applications, for evidence in criminal cases, and to look for threats to U.S. safety and security.

What are the Risks in the Expansion of Biometrics Programs?

Privacy

As a result of data sharing between agencies, biometric data collected for non-criminal purposes, such as immigration-related records, are combined with and 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), it can perpetuate racially motivated targeting of immigrant communities. 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.

If biometrics become standardized, they could replace social security numbers as the primary form of identification. 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. Data standardization also increases the ability of government or private companies to locate and track a given person throughout their lives.

DNA presents privacy issues different from those involved in other biometrics collection. 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. As one circuit court has recognized, "[t]he concerns about DNA samples being used beyond identification purposes are real and legitimate."

Erroneous Data

Data fluidity within and among federal, state, and local agencies can increase the probability that data inaccuracies—such as notoriously inaccurate and out-of-date immigration records—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.

Facial recognition technology can lead to a particularly high rate of false positives. 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." The researchers concluded that an accurate face recognition system will not be an "operational reality for the foreseeable future."

Refugees and Deportations

Data-sharing agreements with other countries mean that receiving governments will immediately know the identity of people deported from the U.S., possibly putting them at risk. Immigration and Customs Enforcement (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. This kind of biometrics sharing could prove disastrous for repatriated refugees or immigrants from countries with a history of ethnic cleansing.

What Legal Protections Exist to Regulate Collection and Use of 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.

Courts have found that the government's interest in protecting United States borders justifies a broad exception to the Fourth Amendment's warrant requirement. 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). 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.

A case recently decided by the Supreme Court, *United States v. Jones*, could provide some insight into how courts might 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. The fact that several members of the Court were willing to reexamine the reasonable expectation of privacy test in light of newly intrusive technology could prove important for future legal challenges to biometrics collection.

What Can Be Done to Maintain Privacy as Biometrics Programs Expand?

This report identifies several principles 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-protection principles:

- **Limit the collection of biometrics** to the minimum necessary to achieve the government's stated purpose.
- **Define clear rules on the legal process required for collection**, such as a court order or a warrant; collection and retention should be specifically disallowed without legal process.
- **Limit the amount and type of data stored** to avoid the retention of data beyond identification and limit the collection of identifying information from people unrelated to the investigation.
- **Limit the combination of more than one biometric in a single database** to keep different types of biometric data in separate databases and to keep biometric data separate from non-biometric, contextual data.
- **Limit data retention times** to a period no longer than necessary to achieve the goals of the program.
- **Define clear rules for use and sharing** so that biometrics collected for one purpose are not used for another purpose.
- **Enact robust security procedures to avoid data compromise**.
- **Mandate notice procedures** to alert people to the fact that their biometrics have been collected.
- **Define and standardize audit trails and accountability throughout the system** so that all database transactions, including biometric input, access to and searches of the system, data transmission, etc. are logged and recorded in a way that assures accountability.
- **Ensure independent oversight** so that every entity that collects or uses biometrics is subject to meaningful oversight from an independent entity.

For more information on biometric data collection, read the full report, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond.*