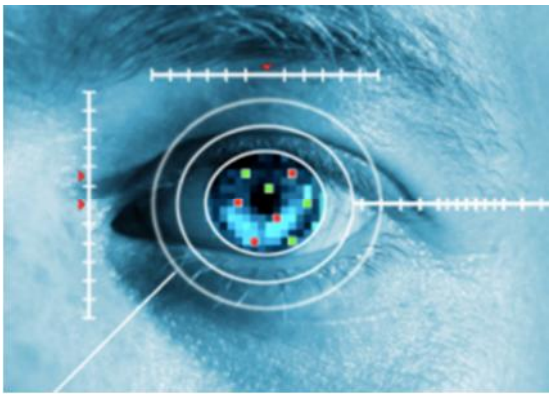
M. Mandl

# 5 Things You Should Know About the FBI's Massive New Biometric Database

*Civil libertarians worry about the roll-out of Next Generation Identification, a massive expansion of the agency's current biometric database.*

*January 8, 2012*



The FBI claims that their fingerprint database (IAFIS) is the "largest biometric database in the world," containing records for over a hundred million people. But that's nothing compared to the agency's plans for Next Generation Identification (NGI), a massive, billion-dollar upgrade that will hold iris scans, photos searchable with face recognition technology, palm prints, and measures of gait and voice recordings alongside records of fingerprints, scars, and tattoos.

Ambitions for the final product are candidly spelled out in an agency report: "The FBI recognizes a need to collect as much biometric data as possible within information technology systems, and to make this information accessible to all levels of law enforcement, including International agencies." (A stack of documents related to NGI was obtained by the Center for Constitutional Rights and others after a FOIA lawsuit.)

It'll be "Bigger -- Better -- Faster," the FBI brags on their Web site. Unsurprisingly, civil libertarians have concerns about the privacy ramifications of a bigger, better, faster way to track Americans using their body parts.

"NGI will expand the type and breadth of information FBI keeps on all of us," says Sunita Patel of the Center for Constitutional Rights. "There should be a balance between gathering information for law enforcement, and gathering information for its own sake."

Here are 5 things you should probably know about NGI:

**1. Face Recognition**

This month, the FBI is giving police departments in 4 states access to face recognition technology that lets them search the agency's mugshot database with only an image of a face. Police can repay the favor by feeding the FBI mugshots they collect from local arrests, bulking up the agency's database with images of more and more people.

The face recognition pilot program is supposed to expand to police departments across the country by 2014. When it's fully operational, the FBI expects its database to contain as many records of faces as there are fingerprints in the current database -- about 70 million, reports Nextgov.com. The agency's optimism seems warranted. If most local police departments are agreeable about information-sharing NGI can vacuum up images from all over the country.

The problem with that, civil libertarians point out, is that anyone's picture can end up in the database, regardless of whether or not they've committed a crime. Mug shots get snapped when people are arrested, and unlike a fingerprint -- which requires either arrest or consent to a background check -- a face could potentially be captured and fed into a database from anywhere.

"Anybody walking around could potentially be entered," Jennifer Lynch, a staff attorney at the Electronic Frontier Foundation, tells AlterNet. "Just the fact that those images can be taken surreptitiously raises concerns. If someone takes your fingerprints, you know. But in the face recognition context, it's possible for law enforcement to collect that data without knowledge." The millions of private and public security cameras all over the country would certainly provide a fruitful source for images, Lynch points out.

Going out in public naturally entails the risk that someone will see what you're doing or take your picture. Law enforcement officials angling for looser surveillance rules often deploy the argument that what people do in public is inherently *not* private. (It's also been used in recent debates over whether it's legal for police to put a GPS tracking device on someone's car without a warrant.) But privacy advocates counter that modern surveillance technology goes so far beyond the human eye, which obviously has neither the capacity to track someone's location for days (GPS) or store their image in a database (video surveillance, face recognition) that traditional distinctions between public and private don't really apply.

An agency powerpoint presented at a 2011 biometrics conference outlines some of the sophisticated technology in the FBI's face recognition initiatives. There's software that distinguishes between twins; 3-D face capture that expands way beyond frontal, two-dimensional mugshots; face-aging software; and automated face detection in video. The report also says agencies can ID individuals in "public datasets," which privacy advocates worry could potentially include social media like Facebook.

Meanwhile, existing laws are rarely up to speed with galloping technological advances in surveillance, say privacy advocates. At this point, "You just have to rely on law enforcement to do the right thing," Lynch says.

**2. Iris Scans**

Iris-scanning technology is the centerpiece of the second-to-last stage in the roll-out of NGI (scheduled for sometime before 2014). Iris scans offer up several advantages to law enforcement, both in terms of identifying people and fattening up databases.

The pattern of an iris is so unique it can distinguish twins, and it allegedly stays the same throughout a person's life. Like facial recognition, iris scans cut out the part where someone has

to be arrested or convicted of a crime for law enforcement to grab a record of their biometric data.

"This capability has the
potential to benefit law enforcement by requiring less interaction with subjects and will allow quicker acquisition," reads a CJIS report to the White House Domestic Policy Council.

In fact, being in the same place as a police officer equipped with a mobile iris-scanning device is all it takes. Last fall, police departments across the country got access to the MORIS device, a contraption attached to an iPhone that lets police collect digital fingerprints, run face recognition and take iris scans. (Over the summer, the FBI also starting passing out mobile devices to local law enforcement that lets them collect fingerprints digitally at the scene, according to Government Computer News.)

**3. Rap-Back System**

A lot of the action in the FBI's fingerprint database is in background checks for job applicants applying to industries that vet for criminal history, like taking care of the elderly or children, hospital work, and strangely, being a horse jockey in Michigan. As Cari Athens, writing for the Michigan Telecommunications and Law Review points out, if a job applicant checks out, the FBI either destroys the prints or returns them to the employer. But that's no fun if the goal is to collect vast amounts of biometric data!

Through the "Rap-Back" system, the FBI will offer employers another option: the agency is willing to keep the fingerprints in order to alert the employer if their new hire has run-ins with the law at any point in the future.

"The Rap-Back Service will provide authorized users the capability to receive notification of criminal and, in limited cases, civil activity of enrolled individuals that occurs after the initial processing and retention of criminal or civil fingerprint transactions," reads the FBI site.

**4. Data Sharing Between Agencies**

The roll-out of NGI advances another goal: breaking down barriers between databases operated by different agencies. One of the directives of the billion-dollar project is to grease information

swapping between the Department of Homeland Security, the State Department, the Department of Justice, and the Department of Defense. The DOJ and DHS have worked toward "interoperatibility" between their databases for years. In 2009, the Department of Defense and DOJ also signed on to an agreement to share biometric information.

All of these agencies have been busy ramping up their collection of data. The Department of Defense's ABIS database has archived fingerprints, images of faces, iris scans, and palm prints in Iraq and Afghanistan and have started collecting voice recordings. They claim to have 5.1 million records, with 49 percent coming from Iraq, but efforts in Afghanistan are ramping up, according to a DoD powerpoint. (Biometric information gathered in Iraq will not be relinquished with our pull-out, as Spencer Ackerman reported.) The Department of Homeland Security biometric database (IDENT) grabs the fingerprints and a photo (searchable with facial recognition) of visitors to the US through a program called US-Visit. Through the Secure-Communities program, meant to reveal the immigration status of people booked in local jails, (more on that below) both IDENT and the FBI collected biometric information from local law enforcement.

A DHS powerpoint about Secure Communities promises that "Under NGI, law enforcement agencies will have the option to search multiple repositories." FBI reports detail how NGI will promote smoother swapping of more and more detailed biometric information: "NGI will increase information processing and sharing needs of the more than 18,000 local, state, federal, and international agencies who are our customers." It's not clear which international agencies will be able to tap into NGI.

The advantages of collaboration are clear, but it's not without some potentially nasty consequences. When that information includes private identifying data, like the unique pattern of an iris, fingerprint or face , civil liberties advocates see likely privacy breaches.

"With more people having access to data, you don't know where data is going, who's using it against you." says EFF's Lynch. "Particularly when you're talking about surreptitious collection like facial recognition, the government has the ability to track you wherever you go. Data sharing between agencies presents the possibility for constant surveillance."

Sunita Patel points out that cases of mistaken identity can be infinitely complicated when the information flows through multiple government agencies. If you're mistakenly flagged by one

agency, she says, how would you go about scrubbing the false record whenever your fingerprint or Iris scan gets pinged by a different one?

**5. NGI and Secure Communities (S-Comm)**

One recent test run in interagency data-sharing has not gone particularly well: Secure Communities, a DHS program that lets local law enforcement officials run the fingerprints of people booked in jails against the IDENT database to check their immigration status and tip off ICE to undocumented immigrants.

Like many policies targeting America's immigrant population, Secure Communities (S-Comm) -- pitched as protection against violent criminals -- devolved into dragnets and mass deportations, with people getting dragged in for minor offenses like missing business permits and even for reporting crimes. In one incident a woman called the police about a domestic violence incident, only to be ensnared in deportation proceedings herself. As Marie Diamond points out in Think Progress, DHS's immigration databases have so many errors that the program "routinely flags citizens as undocumented immigrants."

To complicate matters: activists at the Center for Constitutional Rights argue that the documents they obtained after an FOIA request and lawsuit show that the FBI saw the program as a great opportunity to start beefing up NGI and pushed reluctant local police departments to participate in the program.

An CJIS/FBI guide instructing officials how to pitch S-Comm to local law enforcement explains that, "Ultimately, LEA participation is inevitable because SC is simply the first of a number of biometric interoperatability systems being brought online by the FBI/CJIS 'Next Generation Identification' initiative."

The document lays out strategies for dealing with resistant police departments, including, "Deploy to as many places in the surrounding locale, creating a 'ring of interoperatability' around the resistant site."

"It's a way of operationalizing wide-sweeping intelligence gathering," Sunita Patel of CCR tells AlterNet.

**What could possibly go wrong?**

Advancements in the collection of biometric data are double-edged: there's the threat of a massive government surveillance infrastructure working *too* well -- e.g., surveillance state -- and there are concerns about its weaknesses, especially in keeping data secure.

A breach of a sophisticated, multi-modal biometric database makes for a nightmarish scenario because the whole point of biometric data is that it offers unique ways to ID people, so there's no easy fix -- like a password change -- for compromised biometric data. Pointing to the dangers of identify theft of biometric data, Patel observes that, "Unlike a password, the algorithm of an iris can't be changed."