# Cops to collect more personal data without public notice

**By Ali Winston, Center for Investigative Reporting**

LOS ANGELES – Without notice to the public, Los Angeles County law enforcement officials are preparing to widen what personal information they collect from people they encounter in the field and in jail – by building a massive database of iris scans, fingerprints, mug shots, palm prints and, potentially, voice recordings.

The new database of personal information – dubbed a multimodal biometric identification system – would augment the county's existing database of fingerprint records and create the largest law enforcement repository outside of the FBI of so-called next-generation biometric identification, according to county sheriff's department documents.

On Sept. 15, the FBI announced that the Next Generation Identification System was fully operational. Now that the central infrastructure is in place, the next phase is for local jurisdictions across the country to update their own information-gathering systems to the FBI's standards.

When the system is up and running in L.A., any law enforcement official working in the county, including the Los Angeles Police Department, would collect biometric information on people who are booked into county jails or by using mobile devices in the field.

This would occur even when people are stopped for lesser offenses or pulled over for minor traffic violations, according to documents obtained by the Center for Investigative Reporting through a public records request.

Officials with the sheriff's department, which operates the

countywide system, said the biometric information would be retained indefinitely – regardless of whether the person in question is convicted of the crime for which he or she was arrested.

The system is expected to be fully operational in two or three years, according to the sheriff's department.

All of this is happening without hearings or public input, yet technology companies already are bidding to build the system, interviews and documents show. Officials would not disclose the expected cost of the project or which companies are bidding but said it would be a multimillion-dollar undertaking.

The new system is being readied as the public has become increasingly concerned about privacy invasions by the government, corporations and Internet sources. Privacy advocates worry the public is losing any sense of control over the widespread collection of data on its purchases, travel habits, friendships, health, business transactions and personal communications.

At the same time, cities and counties across the country are facing renewed scrutiny for accepting the transfer of military technology from the Pentagon. The national biometric database is part of the transition of military-grade technologies and information-gathering strategies from the Pentagon to civilian law enforcement. During the wars in Afghanistan and Iraq over the past decade, the U.S. military collected and stored biometric information on millions of civilians and militants.

In 2008, President George W. Bush required the Defense, Homeland Security and Justice departments to establish common standards for collecting and sharing biometric information like iris scans and photos optimized for facial recognition. Law enforcement agencies have been testing mobile systems for documenting biometric information, including a facial

recognition program uncovered in San Diego County last fall.

Authorities in California already collect DNA swabs from arrestees booked into county jails, a practice upheld last year by the U.S. Supreme Court and this year by a federal appeals court in California. Dozens of other states also collect DNA samples from arrestees.

Documents from the Los Angeles County Sheriff's Department show its database will house information on up to 15 million subjects, giving the department a major stake in the Next Generation Identification program, a billion-dollar update to the FBI's national fingerprint database and the largest information technology project in the history of the U.S. Department of Justice.

For privacy advocates, the development of the Los Angeles biometric system without any public oversight or debate and an indefinite data retention policy are causes for concern.

Jeramie Scott, national security counsel for the Electronic Privacy Information Center, said it's critical for the public to be aware that this new technology is being rolled out, because the information held by law enforcement poses unique threats to privacy and anonymity.

"Biometric data is something you cannot change if it is compromised," Scott said. "There are privacy and civil liberties implications that come from law enforcement having multiple ways to identify someone without their consent."

Scott, whose organization has sued the FBI to release information related to Next General Identification, added: "It becomes a one-sided debate when law enforcement alone is making that decision to use new technologies on the public."

Hamid Khan, an organizer with the Stop LAPD Spying Coalition who studies police surveillance, said the arrival of Next Generation Identification means Los Angeles is now a frontier

in the battle for privacy.

“Now our whole bodies are up for grabs,” Khan said.

The multimodal biometric system under development by the sheriff’s department will collect four out of the five “inputs” used by the Next Generation Identification program — fingerprints, mug shots, iris scans and palm prints. Voice recordings are the fifth input.

The L.A. system is designed to transmit and receive data to and from the FBI and the California Department of Justice, which has its own biometric database.

Originally announced in 2008, Next Generation Identification is being rolled out across the country this year after pilot projects were carried out in Michigan, Maryland, Texas, Maine and New Mexico. About 17 million facial records already were integrated into Next Generation Identification as of January.

Earlier this year, residents and city officials in Compton were outraged that Los Angeles County sheriff’s officials had experimented with a cutting-edge aerial surveillance tool known as wide-area surveillance without any prior public notice.

“A lot of people do have a problem with the eye in the sky, the Big Brother, so in order to mitigate any of those kinds of complaints, we basically kept it pretty hush-hush,” sheriff’s Sgt. Douglas Iketani told CIR earlier this year.

Sheriff’s Lt. Joshua Thai, who is in charge of implementing the county’s new biometric database, said the department currently is collecting only fingerprints and has used mobile devices since 2006 to check the fingerprints of people stopped on the street against the county’s records.

Thai said biometric information would be collected from people only when they are arrested and booked, but the mobile devices

would be used to verify individuals' identities in the field.

"It could be somebody gets pulled over for a traffic violation and he or she does not have a driver's license on him or her, and the officer is just trying to identify this person," he said.

Thai said the goal of the project is to help law enforcement officers better identify the people they contact and avoid wrongful arrests. "What we're hoping is that based on the mug shot is that that will compensate some of the biometrics to maybe better identify this person," Thai said.

The sheriff's department declined to release information on which companies were already bidding to install the new system.

According to federal guidelines for the storage of biometric data in Next Generation Identification, information on an individual with a criminal record will be kept until that person is 99 years old. Information on a person without a criminal record will be purged when he or she turns 75.

The FBI's guidelines for keeping biometric data on individuals, regardless of whether they have criminal records, "amounts to an indefinite retention period," said Peter Bibring, a senior staff attorney with the Southern California ACLU. If the Next Generation Identification database simply were an update to the FBI's existing fingerprint database, Bibring said the project wouldn't be problematic.

However, he said the biometric database "significantly expands the type of data law enforcement collects and creates a more invasive system" that may encourage police officers to make more stops in the field to gather photographs and biometric data for the new database.

Experts say the collection and storage of biometric information creates challenges for the legal system and

personal privacy – challenges that have not been adequately considered in the planning and implementation of Next Generation Identification.

Bibring said the new database, if paired with facial recognition-enabled surveillance cameras, could drastically increase law enforcement's ability to track a person's movements just as license-plate readers track vehicles.

"The federal government is creating an architecture that will make it easy to identify where people are and were," Bibring said. "It threatens people's anonymity and ability to move about without being monitored."

Scott, of the Electronic Privacy Information Center, said FBI documents obtained by the center make it clear that uncertainty lingers about who has access to the biometric data that will be stored in the new federal database, and he has doubts regarding the security of such information.

Dozens of Southern California law enforcement agencies have been using mobile fingerprinting devices in the field for roughly a decade. Gang officers routinely submit fingerprints, mug shots and photographs of tattoos and unique scars of suspected gang members to the statewide CalGang database, which contains information on over 130,000 individuals statewide.

The national biometric database also has come under fire from privacy advocates and civil libertarians because it is being implemented without a thorough study of its impact on privacy – which is required by federal law.

"They need to do this before any pilot programs, of which they've done two for facial recognition and iris recognition," Scott said. "They're not meeting their legal obligations, which is now being followed up by state and local authorities."

Khan, of the Stop LAPD Spying Coalition, said such sensitive information in the hands of the Los Angeles County Sheriff’s Department raises further questions about oversight and information security.

“When we look at the multiple contractors and subcontractors and who will have access to this information,” he said, “the whole issue of identity theft comes to mind.”