July 6, 2011 Fact Sheet

SECURE COMMUNITIES AND NEXT GENERATION IDENTIFICATION: The FBI's "Big Brother" Surveillance Agenda

Documents disclosed as a result of Freedom of Information Act (FOIA) litigation by the Center for Constitutional Rights (CCR), the National Day Laborer Organizing Network (NDLON) and the Cardozo Law School Immigration Justice Clinic reveal that Secure Communities goes far beyond immigration enforcement. The program is part of a larger secretive information-collection project that profoundly undermines democracy and liberty.

Secure Communities (S-Comm) is a Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) program introduced in 2008 that links the DHS/ICE immigration databases with the Federal Bureau of Investigation's (FBI) criminal database. With S-Comm, each time a local, state, or tribal police officer conducts a routine criminal background check on a person, they automatically transfer that individual's personal information to DHS. The documents reveal that S-Comm is an integral part of the FBI's Next Generation Identification (NGI) project. NGI will drastically change the landscape of civil liberties and civil rights as related to a person's identity and the ability to prove identity. Through S-Comm, NGI is already being used to detain and deport large numbers of suspected non-citizens.

The newly disclosed documents expose the FBI's goal to accumulate a large biometric database that far exceeds its current fingerprint collection, extending to the collection and retention of iris scans and digital photographs to support automated facial recognitionscans in real-time.[1] NGI aims to impose an automated process linking state and local databases with a federal government biometric data warehouse.[2]

The FBI describes S-Comm as "the first of a number of biometric interoperability systems" that merge into NGI.[3] The FOIA documents show that the FBI, and not DHS, was the first federal agency to call for mandatory implementation of S-Comm. The documents further reveal the FBI's fear that any opt-out for S-Comm might lead states to rightfully question their participation in NGI.[4]

[1] FBI, Next Generation Identification, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Jul. 5, 2011).
[2]FBI-SC-1333-1336, CJIS Advisory Policy Board, Staff Paper, Jun. 4, 2009 (explaining the concept of Record Linking). All documents cited herein were obtained through the federal lawsuit *NDLON et al. v. ICEet al*., 10-cv-3488 (SAS) and are available here: http://uncoverthetruth.org/foia-documents/foia-ngi/ngi-documents/.
[3] FBI-SC-2246-2261 at 2256, FBI/CJIS/US-Visit Deployment Outreach Deep Dive: Creating SC champions in the AOR
[4]*Id.*

What is Next Generation Identification?

NGI will replace the FBI's current system, IAFIS (the Integrated Automated Fingerprint Identification System), which is the world's largest biometric fingerprint database. NGI, however, goes beyond collecting and disclosing fingerprints. Through NGI, the FBI expands personal information collection to other types of biometrics including palm print scans, iris scans, and scar, mark, tattoo, and facial recognition.[5] NGI also expands the disclosure of personal information between federal agencies to an unprecedented degree. Through NGI, any time an individual provides biometric information to one federal agency, that information, without the person's knowledge, becomes accessible to other federal agencies. NGI is slowly but steadily building a massive, easily searchable national database of personal identifying information.

How would NGI Work?

NGI will collect a variety of different biometrics, including fingerprints, iris scans and facial, scar and voice recognition. Whenever a person encounters a federal agency that collects their information (i.e. fingerprints) the NGI system will check its databases. If there is a "match", then a link, or "biometric link identifier" between the agencies is created for this individual. However, the data collection process does not necessarily require the knowledge or cooperation of the individual. Personal data will not only be collected at arrests, but also at crime scenes through latent prints. NGI will also involve widespread use of "FBI Mobile," a form of technology first used by the military that will allow for the collection of biometric samples in the field, without an arrest.[6]

Why Should You Be Concerned About NGI?

NGI invades our privacy and puts our personal information at risk

The 1974 Privacy Act restricts federal agencies from disclosing personally identifiable information and requires that they maintain records with accuracy and diligence. Yet the FBI claims that it is exempt from both of these provisions. As reported by the Washington Post, in response to a 2004 Electronic Privacy Information Center objection to its exemption of the National Crime Information Center database from the Privacy Act, the FBI stated, "It is impossible to determine in advance what information is accurate, relevant, timely and complete."[7] The Privacy Act itself includes a "law enforcement" exception that allows the disclosure of personally identifiable information "upon receipt of a written request, [to] disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity." With this mindset, the federal government is not able to adequately protect our private identifying information.

Equally concerning is that the accumulation of information in such large databases creates targets for hackers, disgruntled insiders, and national enemies. Information collection projects like NGI greatly endanger national security and leave us vulnerable to identity theft. Using biometric link identifiers introduces the risk that information gathered for one purpose will be used for completely unrelated, purposes, without our knowledge or consent, and in blatant violation of our privacy rights.

---

[5] FBI, Next Generation Identification, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Jul. 5, 2011).
[6] FBI-SC-1232-1240, at 1237, CJIS Advisory Policy Board, Staff Paper, Working Group Meetings, Informational Topic, Spring 2010.
[7] Ellen Nakashima, WASHINGTON POST, *FBI Prepares Vast Database of Biometrics: $1Billion Project to Include Images of Irises and Faces*, Dec. 22, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html.

The FBI has been rolling-out NGI with little transparency or public dialogue

The FBI is now publicly taking the position that states and localities cannot opt-out or limit their participation in S-Comm.[8] But the documents make clear that the FBI was concerned about resistance to S-Comm from the outset. This is why the FBI adopted the confusing S-Commopt out policy that allowed local agencies to opt out of receiving information but still required them to send information to federal agencies.[9] The FBI decided, though waited to disclose to states and the public until much later, that participation in S-Comm would be mandatory.[10] Many details about the scope, impact, and process of NGI and the legal basis for the FBI's policies are still unknown and have not been scrutinized by the media or the public.

NGI targets vulnerable communities first

The test subjects for this new system are the most vulnerable populations, like immigrants, but ultimately everyone will be impacted. The recent experiences of individuals within immigrant communities are examples of some the consequences when government agencies are given unfettered access to information for purposes different than the reasons for which the information was initially collected.

Maria Bolanos called the police after a fight with her partner, trusting they would help her. Instead, the police turned her over to deportation officers following a S-Comm "match." She is now fighting to remain in the country with her children. Other victims of domestic violence hear of Maria's story and the many others like her, and chose not to reach out to the authorities for the help that they need, due to the fear that the information will be disclosed to immigration authorities.

NGI is driven by profit

In 2008, Lockheed Martin, the largest federal contractor, won a billion dollar contract with the FBI to work on NGI. The contract has the potential for up to nine option years. Lockheed Martin is invested in information gathering and disclosure. Despite the concerns identified above, pressure to use biometrics is driven by the biometric industry, which is driven by profit, rather than a reasoned analysis of the dangers of such policies.

No database or technology is error-proof

NGI will transform the scope of information stored, monitored and disclosed by the federal government. With immense quantities of valuable, personal information, it is an attractive target for identity thieves. It is also susceptible to bureaucratic mistakes and malicious or fraudulent use. Unlike other databases, a mistake in the NGI database would carry huge repercussions. If someone steals or corrupts the information linked to your fingerprint, your identity could be lost forever. Even worse, an attack on the centralized NGI database could seriously compromise sensitive material and our national security.

NGI also highlights the risks associated with collecting latent biometrics. Latent biometric data is biometric evidence (e.g. fingerprints, DNA) left behind at a crime scene or otherwise collected without an attached identity. Latent biometric data will remain in the NGI database to be matched against future collected data. Attempting to make a latent match can be difficult and lead to misidentifications because latent prints are often small, distorted, smudged or otherwise unclear.

---

[8] *See e.g.*, MirelaIverac, WNYC, *NY Can't Opt-Out of Fingerprint Sharing with Feds*, Jun. 27, 2011, *available at* http://www.wnyc.org/articles/wnyc-news/2011/jun/27/secure-communities/.

[9] FBI-SC-2246-2261 at 2254-2256, 2258, FBI/CJIS/US-Visit Deployment Outreach Deep Dive: Creating SC champions in the AOR;FBI-SC-1333-1336, CJIS Advisory Policy Board, Staff Paper, June 4, 2009.

[10] FBI-SC-2246-2261 at 2256, FBI/CJIS/US-Visit Deployment Outreach Deep Dive: Creating SC champions in the AOR; FBI-SC-1333-1336 CJIS Advisory Policy Board, Staff Paper, June 4, 2009.

Brandon Mayfield, an American-born convert to Islam, was misidentified by the FBI to be responsible for the 2004 Madrid train bombing after his fingerprints were compared to latent fingerprints from the crime scene. The FBI initially reported there was an "absolutely incontrovertible match" and that it was a "100 percent positive" match. Mayfield spent two weeks in police custody before being released.

In 2008 Mark Lyttle, a U.S. citizen, was wrongly categorized as an undocumented immigrant even after he signed sworn statements indicating he was born in North Carolina. This mistake occurred when Mr. Lyttle was being processed for a misdemeanor and an intake clerk typed "Mexico" as the place of birth. Instead of confirming any of the information, officials deported Mr. Lyttle. After four months of being stateless and sent to five countries in Latin America, Mr. Lyttle's U.S. citizenship was confirmed by a Guatemalan official.

The agencies may collect information in their databases on people who do not match any pre-existing data held by the agencies. This information would be kept without the consent or knowledge of the person, subject to compromise or for use in tracking or targeting the person at a later time.

NGI is a form of extreme "Big Brother" surveillance and introduces a new system of policing

The government's past unsuccessful plan to issue national IDs was met with forceful opposition. NGI is the FBI's back-door attempt to advance its agenda to increase surveillance. With NGI, the FBI is distorting existing laws and systems to intrude into the lives of every-day people and offend the ideals of freedom, privacy and democracy that we think we can take for granted.

NGI, through S-Comm and its other components, turnslocal police into federal officers, potentially exposing us all to intrusive surveillance and tracking, to be targeted by government programs that we may not even know about.