US ISN'T COLLECTING ONLY ELECTRONIC DATA ON YOU — HUGE BIOMETRIC DATABASE UNDER CONSTRUCTION, TOO

Edward Snowden's revelations have shed much light on how secret government programs are collecting huge amounts of telephone, email and other electronic data generated by every US citizen even though, as Marcy has shown repeatedly, claims that collecting all of this data have enabled the capture of terrorists turn out to be significantly overblown. Sadly, it's not just records of our communications that the government is collecting. The FBI is taking the lead in putting together what it calls Next Generation Identification. This program will expand the conventional FBI fingerprint database to include significant amounts of biological, or biometric data. From the FBI's own description:

> The future of identification systems is currently progressing beyond the dependency of a unimodal (e.g., fingerprint) biometric identifier towards multimodal biometrics (i.e., voice, iris, facial, etc.). The NGI Program will advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multimodal system that will facilitate biometric fusion identification techniques. The framework will be expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems. Once developed and implemented, the NGI initiatives and multimodal functionality will promote a high level of information

> sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification.

Wait. See that “etc.” in the “voice, iris, facial, etc”? Given the government’s behavior on electronic data, throwing in an “etc.” on biometric data is pretty unnerving. Impressive work is being done by the Electronic Privacy Information Center to shed light on just what the government is up to with Next Generation Identification. Here is their description of the program:

> The Federal Bureau of Investigation is developing a biometric identification database program called “Next Generation Identification” (NGI). When completed, the NGI system will be the largest biometric database in the world. The vast majority of records contained in the NGI database will be of US citizens. The NGI biometric identifiers will include fingerprints, iris scans, DNA profiles, voice identification profiles, palm prints, and photographs. The system will include facial recognition capabilities to analyze collected images. Millions of individuals who are neither criminals nor suspects will be included in the database. Many of these individuals will be unaware that their images and other biometric identifiers are being captured. Drivers license photos and other biometric records collected by civil service agencies could be added to the system. The NGI system could be integrated with other surveillance technology, such as Trapwire, that would enable real-time image-matching of live feeds from CCTV surveillance cameras. The Department of Homeland Security has expended hundreds of millions of dollars to establish state and local surveillance systems, including CCTV cameras that record the

> routine activities of millions of individuals. There are an estimated 30 million surveillance cameras in the United States. The NGI system will be integrated with CCTV cameras operated by public agencies and private entities.

So just as the government has moved far beyond tapping communications only with a warrant to include the communications of innocent civilians, biometric identifiers of innocent civilians will be included in NGI alongside identifiers of known criminals. And what could possibly go wrong with our information being assembled in this way? Here's how EPIC says the database will be built and maintained:

> The NGI database will be used for both law enforcement and non-law enforcement purposes. It will be available to law enforcement agencies at the local, state, and federal level. But it will also be available to private entities, unrelated to a law enforcement agency. Using facial recognition on images of crowds, NGI will enable the identification of individuals in public settings, whether or not the police have made the necessary legal showing to compel the disclosure of identification documents. The New York City Police Department began scanning irises of arrestees in 2010; these sorts of records will be entered into NGI. The Mobile Offender Recognition and Information System ("MORIS"), a handheld device, allows officers patrolling the streets to scan the irises and faces of individuals and match them against biometric databases. Similarly, children in some school districts are now required to provide biometric identifiers, such as palm prints, and are also subject to vein recognition scans. Clear, a private company offering identity services based on biometric

> identifiers, attempted to sell the biometric database of its users after its parent company, Verified Identity Pass, declared bankruptcy. The transfer of the biometric database was blocked by a federal district court judge.
>
> There is a substantial risk that personally identifiable information could be lost or misused as a result of the creation of the NGI system. Among the private contractors involved in the deployment of NGI are Lockheed Martin, IBM, Accenture, BAE Systems Information Technology, Global Science & Technology ("GST"), Innovative Management & Technology Services ("IMTS"), and Platinum Solutions. Arizona, Hawaii, Kansas, Maryland, Michigan, Missouri, Nebraska, New Mexico, Ohio, South Carolina, and Tennessee are actively participating in the NGI program. The FBI is pursuing an aggressive deployment of the NGI program, scheduled for completion and full deployment by 2014.

Okay, then. A huge program, costing hundreds of millions of dollars, is being assembled by the same cast of government contractors who have given us decades of cost-overruns and defective products. And they might even give access to the system to private entities? Wow.

Of course, we are expected to believe that this system will work just as it already does on NCIS when Abby or McGee puts a photo into their computer and the identity of the terrorist pops up five seconds later. But in a 300+ page document (pdf) EPIC obtained under FOIA, we have this little nugget that tells us the current state of the art when it comes to facial recognition software:

> NGI shall return an incorrect candidate a maximum of 20% of the time.

Think about that. In putting out the specifications for the system to be developed (and that is planned to be implemented next year!), the government is willing to get for its huge investment a system that makes a false positive identification one in five times. That could put a very large number of entirely innocent people in a huge pile of trouble very quickly.

The problem is that current technology on facial recognition requires very high quality photographs, preferably full face, for identification to work. That is why it took so long to identify the Tsarnaev brothers even though surveillance photos had been found and both of them had identification photos in the database that was searched.

Putting NGI into full functionality before facial recognition software is ready and with so many innocent civilians in the database is a huge recipe for disaster. And of course, you can rest assured that the government will have built immunity into the system for both itself and the contractors responsible for building the system. I'm assuming that the victims of the false positive identifications will have little to no recourse in recovering the huge expenses they will face in proving their innocence. Many more lives are soon to be ruined at the expense of security theater.

I've just started reading up on Next Generation Identification, but from what I've seen so far, it looks to me like the biometric database is going to be a perfect clone of the electronic databases: huge haystacks that are incredibly expensive and of very limited to no value when most in need of producing results.