RT QUESTION MORE.

FBI begins installation of $1 billion face recognition system across America

Published: 8 September, 2012

Birthmarks, be damned: the FBI has officially started rolling out a state-of-the-art face recognition project that will assist in their effort to accumulate and archive information about each and every American at a cost of a billion dollars.

The Federal Bureau of Investigation has reached a milestone in the development of their Next Generation Identification (NGI) program and is now implementing the intelligence database in unidentified locales across the country, New Scientist reports in an article this week. The FBI first outlined the project back in 2005, explaining to the Justice Department in an August 2006 document (.pdf) that their new system will eventually serve as an upgrade to the current Integrated Automated Fingerprint Identification System (IAFIS) that keeps track of citizens with criminal records across America .

"The NGI Program is a compilation of initiatives that will either improve or expand existing biometric identification services," its administrator explained to the Department of Justice at the time, adding that the project, *"will accommodate increased information processing and sharing demands in support of anti-terrorism."*

"The NGI Program Office mission is to reduce terrorist and criminal activities by improving and expanding biometric identification and criminal history information services through research, evaluation and implementation of advanced technology within the IAFIS environment."

The agency insists, *"As a result of the NGI initiatives, the FBI will be able to provide services to enhance interoperability between stakeholders at all levels of government, including local, state, federal, and international partners."* In doing as such, though, the government is now going ahead with linking a database of images and personally identifiable information of anyone in their records with departments around the world thanks to technology that makes fingerprint tracking seem like kids' stuff.

According to their 2006 report, the NGI program utilizes *"specialized requirements in the Latent Services, Facial Recognition and Multi-modal Biometrics areas"* that *"will allow the FnewBI to establish a terrorist fingerprint identification system that is compatible with other systems; increase the accessibility and number of the IAFIS terrorist fingerprint records; and provide latent palm print search capabilities."*

Is that just all, though? During a 2010 presentation (.pdf) made by the FBI's Biometric Center of Intelligence, the agency identified why facial recognition technology needs to be embraced. Specifically, the FBI said that the technology could be used for *"Identifying* *subjects in public datasets,"* as well as *"conducting automated surveillance at lookout locations"* and *"tracking subject movements,"* meaning NGI is more than just a database of mug shots mixed up with fingerprints — the FBI has admitted that this their intent with the technology surpasses just searching for criminals but includes spectacular surveillance capabilities. Together, it's a system unheard of outside of science fiction.

New Scientist reports that a 2010 study found technology used by NGI to be accurate in picking out suspects from a pool of 1.6 million mug shots 92 percent of the time. The system was tested on a trial basis in the state of Michigan earlier this year, and has already been cleared for pilot runs in Washington, Florida and North Carolina. Now according to this week's New Scientist report, the full rollout of the program has begun and the FBI expects its intelligence infrastructure to be in place across the United States by 2014.

In 2008, the FBI announced that it awarded Lockheed Martin Transportation and Security Solutions, one of the Defense Department's most favored contractors, with the authorization to design, develop, test and deploy the NGI System. Thomas E. Bush III, the former FBI agent who helped develop the NGI's system requirements, tells NextGov.com*, "The idea was to be able to plug and play with these identifiers and biometrics.*" With those items being collected without much oversight being admitted, though, putting the personal facts pertaining to millions of Americans into the hands of some playful Pentagon staffers only begins to open up civil liberties issues.

Jim Harper, director of information policy at the Cato Institute, adds to NextGov that investigators pair facial recognition technology with publically available social networks in order to build bigger profiles. Facial recognition "*is more accurate with a Google or a Facebook, because they will have anywhere from a half-dozen to a dozen pictures of an individual, whereas I imagine the FBI has one or two mug shots,"* he says. When these files are then fed to law enforcement agencies on local, federal and international levels, intelligence databases that include everything from close-ups of eyeballs and irises to online interests could be shared among offices.

The FBI expects the NGI system to include as many as 14 million photographs by the time the project is in full swing in only two years, but the pace of technology and the new connections constantly created by law enforcement agencies could allow for a database that dwarfs that estimate. As RT reported earlier this week, the city of Los Angeles now considers photography in public space "suspicious," and authorizes LAPD officers to file reports if they have reason to believe a suspect is up to no good. Those reports, which may not necessarily involve any arrests, crimes, charges or even interviews with the suspect, can then be filed, analyzed, stored and shared with federal and local agencies connected across the country to massive data fusion centers. Similarly, live video transmissions from thousands of surveillance cameras across the country are believed to be sent to the same fusion centers as part of TrapWire, a global eye-in-the-sky endeavor that RT first exposed earlier this year.

"Facial recognition creates acute privacy concerns that fingerprints do not," US Senator Al Franken (D-Minnesota) told the Senate Judiciary Committee's subcommittee on privacy, technology and the law earlier this year. *"Once someone has your faceprint, they can get your name, they can find your social networking account and they can find*

and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online."

In his own testimony, Carnegie Mellon University Professor Alessandro Acquisti said to Sen. Franken, *"the convergence of face recognition, online social networks and data mining has made it possible to use publicly available data and inexpensive technologies to produce sensitive inferences merely starting from an anonymous face."*

"Face recognition, like other information technologies, can be source of both benefits and costs to society and its individual members," Prof. Acquisti added. "*However, the combination of face recognition, social networks data and data mining can significant undermine our current notions and expectations of privacy and anonymity."*

With the latest report suggesting the NGI program is now a reality in America, though, it might be too late to try and keep the FBI from interfering with seemingly every aspect of life in the US, both private and public. As of July 18, 2012, the FBI reports, *"The NGI program … is on scope, on schedule, on cost, and 60 percent deployed."*