GlobalResearch
Center for Research on Globalization

FBI's Facial Recognition Program Hits 'Full Operational Capability'

By RT
Global Research, September 16, 2014
RT

Region: USA
Theme: Police State & Civil Rights

The Federal Bureau of Investigation's Next Generation Identification System, a biometric database reliant on tens of millions of facial-recognition records, is now fully operational, the agency announced Monday.

The NGI system, after three years of development, is billed by the FBI as a new breakthrough for criminal identification and data-sharing between law enforcement agencies.

"This effort is a significant step forward for the criminal justice community in utilizing biometrics as an investigative enabler," the FBI said in a statement.

The NGI database contains over 100 million individual records that link a person's fingerprints, palm prints, iris scans and facial-recognition data with personal information like their home address, age, legal status and other potentially compromising details.

Perhaps the most controversial aspect of the NGI is the facial-recognition information, which civil liberties advocates have said for years is among the most serious future threats to Americans' privacy. The NGI database is expected to contain 52 million facial-recognition images alone by 2015.

The FBI said Monday that two new features of the database are now complete, capping off the NGI's "operational capability."

One feature, the Rap Back, will allow officials to "receive ongoing status notifications of any criminal history reported on individuals holding positions of trust, such as school teachers."

Additionally, the Interstate Photo System (IPS) facial recognition service "will provide the nation's law enforcement community with an investigative tool that provides an image-searching capability of photographs associated with criminal identities."

But Americans not suspected of any criminal activity could easily be swept up into the NGI, according to the Electronic Frontier Foundation (EFF), in any number of ways. An individual who goes through a fingerprint background check for an employment opportunity, for instance, could soon be required to submit a picture of herself as well.

That picture could be stored alongside images of suspected criminals, unlike fingerprints, where a clear differentiation is made between law-abiding citizens and those who have been in trouble with the law before.

According to EFF senior staff attorney Jennifer Lynch, there is cause for concern because “the FBI and Congress have thus far failed to enact meaningful restrictions on what types of data can be submitted to the system, who can access the data and how the data can be used.”

> “For example, although the FBI has said in these documents that it will not allow non-mug shot photos such as images from social networking sites to be saved from the system, there are no legal or even written FBI policy restrictions in place to prevent this from occurring,” Lynch said.

In June, EFF and other privacy advocates warned that the FBI’s facial-recognition database is in desperate need of more oversight.

“One of the risks here, without assessing the privacy considerations, is the prospect of mission creep with the use of biometric identifiers,” Jeramie Scott of the Electronic Privacy Information Center told National Journal. “It’s been almost two years since the FBI said they were going to do an updated privacy assessment, and nothing has occurred.”

A 2010 report of the FBI’s facial-recognition technology found that it could fail one in every fiveinstances it was used, a rate higher than fingerprinting or iris scans.

Yet FBI Director James Comey has told Congress that the database would not amass photos of innocent people, and that it is only intended to “find bad guys by matching pictures to mugshots.”

In a milestone announcement, the FBI said in August that it had tracked down a 14-year fugitive suspected of child abuse using facial-recognition technology.

Meanwhile, US government intelligence researchers are developing the Janus program, which will“radically expand the range of conditions under which automated face recognition can establish identity.”

There are currently no federal restraints on the use of facial-recognition software.

Articles by: RT