



Written by [Michael Tennant](#) on May 10, 2016

FBI Seeks to Exempt Its Massive Biometric Database From Federal Privacy Law

The Federal Bureau of Investigation (FBI) is developing a [massive database](#) of Americans' biometric information, but it doesn't want the people it supposedly serves to know just what data it has on them or to be able to correct it if it's wrong.

Last Thursday, the Justice Department [proposed](#) exempting the FBI's Next Generation Identification (NGI) System — a database containing fingerprints, iris scans, palm prints, voice data, photographs, and other biometric data on millions of Americans, including many never convicted of any crime — from various provisions of the federal Privacy Act, which “requires federal agencies to share information about the records they collect with the individual subject of those records, allowing them to verify and correct them if needed,” according to [Nextgov](#).



The department claimed that it was taking this action “in order to prevent interference with the FBI's mission to detect, deter, and prosecute crimes and to protect the national security.” Privacy advocates aren't convinced.

{modulepos inner_text_ad}

The proposal, which is open for public comment through June 6, “would set a worrying precedent in which law enforcement has significant leeway to decide what information to collect without informing the subject, according to Jeramie Scott, a national security counsel at the Electronic Privacy Information Center [EPIC], a research group advocating for digital civil liberties,” reported *Nextgov*.

While the FBI claims most of the data in NGI comes from state and local law-enforcement agencies, a significant percentage also comes from criminal-background checks requested by both private and public entities. Many private employers conduct background checks on prospective employees; all federal employees must undergo them. In addition, some states require them for members of certain professions such as child-care workers, doctors, and attorneys. That means millions of Americans never charged with a crime could wind up in NGI with no way of verifying that their records in the database are accurate. (The FBI says those who voluntarily submit fingerprints for background checks receive a legally mandated notice that their information has been forwarded to the agency.)

In its proposal, the FBI argues that letting an individual know he is in the NGI database “would specifically reveal investigative interest by the FBI or agencies that are recipients of the disclosures. Revealing this information could compromise ongoing, authorized law enforcement and national



Written by [Michael Tennant](#) on May 10, 2016

security efforts and may permit the record subject with the opportunity to evade or impede the investigation.”

Furthermore, the FBI claims an exemption from the Privacy Act’s requirement that individuals be permitted to see and amend their records primarily because that, too, could alert the subject of an investigation to the fact that he is being investigated. Also, the agency is concerned, it says, that “providing access” to a subject’s records could “disclose information which would constitute an unwarranted invasion of another’s personal privacy.” Yes, you read that correctly: The FBI is claiming exemption from the Privacy Act because it is worried about invasions of privacy.

Americans need not fear that keeping secret files on them constitutes a threat to their liberties, the Justice Department assures us. “The FBI takes seriously its obligation to maintain accurate records despite its assertion of this exemption,” reads the proposal. Besides, since most of the data in NGI comes from state and local law enforcement, “it would be inappropriate for the FBI to undertake correction or amendment.” What’s more, the agency may even, “in its sole discretion,” deign to allow some people to know about and/or to correct their records.

The Privacy Act further mandates that agencies retain information on individuals only to the extent that doing so is “necessary and appropriate” to achieve their lawful objectives. The FBI, however, cannot be hamstrung in any way from building its database because, according to the proposal, “it is impossible to determine in advance what information is accurate, relevant, timely and complete. With time, seemingly irrelevant or untimely information may acquire new significance when new details are brought to light.”

In addition, the FBI states that “the information may aid in establishing patterns of activity and providing criminal leads.” That, Scott told *Nextgov*, is particularly worrisome.

“We don’t know exactly what that means,” Scott said. “If you have no ability to access the record the FBI has on you, even when you’re not part of an investigation or under investigation, and lo and behold inaccurate information forms a ‘pattern of activity’ that then subjects you to [be] the focus of the FBI, then that’s a problem.”

These concerns are heightened by the FBI’s wall of secrecy surrounding NGI. The agency has tried to keep as much as possible about the database from the public. EPIC was forced to sue to get the contracts and technical requirements about NGI out into the open.

Among the few details known about the system, thanks to the intrepid Electronic Frontier Foundation (EFF) and EPIC, are that the FBI wants to use NGI to track people as they move from one place to another — “perfect tracking is inimical to a free society,” EFF rightly [observed](#) — and that NGI’s facial-recognition database was expected to contain [52 million images](#) by 2015. The specs on the facial-recognition software, by the way, allow for false matches [up to 20 percent of the time](#), making it highly likely that innocent people will be subjected to unwarranted investigations and arrests, particularly given that “law enforcement at all levels ... will be given access to a database that includes noncriminal as well as criminal face images with no limits on how the data can be used,” according to [Law360](#).

The FBI wants all the privacy it can get about NGI, which is ripe for political abuse and identity theft, while denying Americans even the modicum of privacy required by law. That tells us more about NGI and the FBI than all the documents the agency could possibly be forced to cough up — and none of what it says bodes well for the future of the Republic.



Subscribe to the New American

Get exclusive digital access to the most informative, non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.

Subscribe