FBI Fighting to Exempt Biometric Database from the Privacy Act

May 24, 2016 â€“ The FBI has a database that they really donâ€™t want you to be able to review. It consists of biometric data; meaning it contains digitized versions of things like fingerprints, facial scans for facial recognition, DNA and iris scans on millions of people. And the chances that your data may be included in it are probably higher than you think. It is called the Next Generation Identification System (NGIS) and it has some very Orwellian implications.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

You might think that a database such as NGIS would contain information on criminals and those with security clearances. And it does, but that is just the tip of the iceberg.

If you haveâ€¦ or hadâ€¦ a job that required you to submit your fingerprints for a background check, then there is a pretty good chance that you are included in NGIS. Thatâ€™s a huge portion of the population. For instance, if you have ever applied for a professional license â€“ say you are realtor â€“ and had to submit your fingerprints, youâ€™re probably in NGIS. Th same is true if you work for a private sector employer who used any biometric data to run a background check on you.

Anyone who has been arrested and subject to a DNA test and had their mug shot taken is also likely to be in the database. That includes people who never went to trial, may never have been charged with a crime and who were certainly never convicted of a crime.

And of course, if you have been in the military, chances are your data is in NGIS.

What this means is that millions of people can be monitored by the government for absolutely no reason at all.

In our opinion, there are almost too many problems created by NGIS that it would be difficult to catalog them all. But here are a few that need to be considered:

NGIS is a prime target for hackers â€“ If you think thatâ€™s a stretch then just consider that the federal governmentâ€™s Office Personnel Management was hacked last year and lost the biometric data of millions of Americans with security clearances. Time and again, the federal government has proven that they are completely incompetent at protecting stored data.

Without being subject to the Privacy Act, citizens have no way to insure that the data in NGIS is accurate â€“ This is likely to be a real issue going forward. Just think about it. What if some data entry clerk enters incorrect data about you into NGIS? This is a database that the FBI admits using in criminal investigations. The Privacy Act allows you to access your own data and to correct errors. Without that ability, it is easy to see how innocent people could get erroneously caught up in legal proceedings.

Mission creep â€“ The more data that gets included in NGIS, the more tempting it will be for the government to use it. And the government is likely to find as many ways to use NGIS as they can think of exempting this type of database from public scrutiny is simply dangerous in a society where personal liberty is valued. Ideally, congress should place strict limits on the use of NGIS data. But until that happens, public oversight is essential.

The FBI is trying to exempt NGIS using federal rulemaking. The proposed exemption has been published in the Federal Register and public comments are open until June 6th. You can find instructions for submitting comments in the Federal Register article. We are advising our readers to submit comments opposing this exemption.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS