BREAKING: OPM AND DOD (CLAIM THEY) DON'T THINK FINGERPRINT DATABASES ARE ALL THAT USEFUL

In the most negative news dump released behind the cover of Pope Francis' skirts, Office of Public Management just announced that rather than previous reports that 1.1 million people had had their fingerprints stolen from OPM's databases, instead 5.6 million have.

Aside from the big numbers involved, there are several interesting aspects of this announcement.

First, it seems OPM had an archive of records on 4.5 million people, including fingerprint data, they hadn't realized was there at first.

> As part of the government's ongoing work to notify individuals affected by the theft of background investigation records, the Office of Personnel Management and the Department of Defense have been analyzing impacted data to verify its quality and completeness. During that process, OPM and DoD identified archived records containing additional fingerprint data not previously analyzed.

If, as it appears, this means OPM had databases of key counterintelligence lying around it wasn't aware of (and therefore wasn't using), it suggests Ron Wyden's concern that the government is retaining data unnecessarily is absolutely correct.

Rather bizarrely, upon learning that someone found and went through archived databases to

obtain more fingerprint data, “federal experts” claim that “as of now, the ability to misuse fingerprint data is limited.”

As EFF just revealed, since February the FBI has been busy adding fingerprint data it gets when it does when it does background checks on job applicants into its Next Generation Identification database.

> Being a job seeker isn’t a crime. But the FBI has made a big change in how it deals with fingerprints that might make it seem that way. For the first time, fingerprints and biographical information sent to the FBI for a background check will be stored and searched right along with fingerprints taken for criminal purposes.
>
> The change, which the FBI revealed quietly in a February 2015 Privacy Impact Assessment (PIA), means that if you ever have your fingerprints taken for licensing or for a background check, they will most likely end up living indefinitely in the FBI’s NGI database. They’ll be searched thousands of times a day by law enforcement agencies across the country—even if your prints didn’t match any criminal records when they were first submitted to the system.
>
> This is the first time the FBI has allowed routine criminal searches of its civil fingerprint data. Although employers and certifying agencies have submitted prints to the FBI for decades, the FBI says it rarely retained these non-criminal prints. And even when it did retain prints in the past, they “were not readily accessible or searchable.” Now, not only will these prints—and the biographical data included with them—be available to any law enforcement agent who wants to look for them, they will be searched as a matter of course along with all prints

> collected for a clearly criminal purpose (like upon arrest or at time of booking).

In its PIA explaining the move, FBI boasts that this will serve as "an 'ongoing' background check that permits employers, licensors, and other authorized entities to learn of criminal conduct by a trusted individual." To suggest that a massive database of fingerprints can provide the FBI real-time updates on certain behaviors, but pretend it wouldn't serve a similar purpose to the Chinese, defies logic. Heck, why is OPM keeping fingerprint information if it can't be used? And of course, all that assumes none of the 5.6 million people affected has a fingerprint-authenticating iPhone.

Of course this can be used, otherwise the Chinese wouldn't have gone out of their way to get it!

But OPM's claim that the Chinese just went out of their way to get that fingerprint data for no good reason provides the agency with a way to delay notification while FBI, DHS, DOD and "other members of the Intelligence Community" come up with ways to limit the damage of this.

> If, in the future, new means are developed to misuse the fingerprint data, the government will provide additional information to individuals whose fingerprints may have been stolen in this breach.

After which OPM spends two paragraphs talking about the identity protection those whose identities have been stolen will get, as if that mitigates a huge counterintelligence problem.

It sure sounds like OPM is stalling on informing the people who've been exposed about how badly they've been exposed, under the incredible claim that databases of fingerprints aren't all that useful.