US PERSONS ON MILITARY INTELLIGENCE SHARING DATABASES

Steven Aftergood catches Charles McCullough, the Intelligence Community Inspector General who has resisted exercising oversight over spying, doing his job.

> "A civilian employee with the Army Intelligence and Security Command made an IC IG Hotline complaint alleging an interagency data repository, believed to be comprised of numerous intelligence and non-intelligence sources, improperly included U.S. person data," the IC IG wrote. "The complainant also reported he conducted potentially improper searches of the data repository to verify the presence of U.S. persons data. We are researching this claim."

Given prior reports about ICREACH — which purportedly focuses on foreign collected data but therefore would include US person data collected overseas — this is not that surprising. (I don't think this should be ICREACH, however, because that's not explained as a repository.)

But I find it particularly interesting that this complaint comes from someone at INSCOM, the Army intelligence outfit where Keith Alexander tried to ingest US person data in 2001, only to have Mikey Hayden refuse (!).

> The heartburn first flared up not long after the 2001 terrorist attacks. Alexander was the general in charge of the Army's Intelligence and Security Command (INSCOM) at Fort Belvoir, Virginia. He began insisting that the NSA give him raw, unanalyzed data about suspected terrorists from the agency's massive digital cache, according to

> three former intelligence officials. Alexander had been building advanced data-mining software and analytic tools, and now he wanted to run them against the NSA's intelligence caches to try to find terrorists who were in the United States or planning attacks on the homeland.
>
> By law, the NSA had to scrub intercepted communications of most references to U.S. citizens before those communications can be shared with other agencies. But Alexander wanted the NSA "to bend the pipe towards him," says one of the former officials, so that he could siphon off metadata, the digital records of phone calls and email traffic that can be used to map out a terrorist organization based on its members' communications patterns.
>
> "Keith wanted his hands on the raw data. And he bridled at the fact that NSA didn't want to release the information until it was properly reviewed and in a report," says a former national security official. "He felt that from a tactical point of view, that was often too late to be useful."
>
> Hayden thought Alexander was out of bounds. INSCOM was supposed to provide battlefield intelligence for troops and special operations forces overseas, not use raw intelligence to find terrorists within U.S. borders. But Alexander had a more expansive view of what military intelligence agencies could do under the law.
>
> "He said at one point that a lot of things aren't clearly legal, but that doesn't make them illegal," says a former military intelligence officer who served under Alexander at INSCOM.
>
> In November 2001, the general in charge

> of all Army intelligence had informed his personnel, including Alexander, that the military had broad authority to collect and share information about Americans, so long as they were "reasonably believed to be engaged" in terrorist activities, the general wrote in a widely distributed memo.

Indeed, given the timing (IC IG's report describes this as happening in the fourth quarter of calendar year 2013, so in the months after this Shane Harris report), it's possible this report is what led the tipster to check whether US person data was available in repositories available to INSCOM.

While INSCOM focuses on battlefield intelligence, it also does cybersecurity and force protection, the kind of thing that has, in the past, targeted Americans (even Americans peddling porn!). So while this might just reflect oversharing, it also might reflect a return to the mentality of Keith Alexander.