



## 'Technical irregularities' plagued contact chaining at NSA

Derek B. Johnson

December 9, 2019

An intelligence official offered new insights into technical problems that have plagued a controversial spying program and led the National Security Agency to over-collect hundreds of millions of unauthorized communication records.

The Privacy and Civil Liberties Oversight Board (PCLOB) had indicated it is actively reviewing the NSA's Call Detail Records program authorized under the 2015 USA Freedom Act. At a Dec. 6 Cato Institute conference, Ben Huebner, chief civil liberties and privacy officer for the Office of the Director of National Intelligence, said that review was in the final stages of approval before completion.

"The [Board] is concluding a review of this program, and we're actually actively doing a declassification review," Huebner said. "So more will be coming out ... there will be a lot more coming out on this."

That review, which will examine the operational use and implementation challenges surrounding the program, is expected to provide more detail behind the "technical irregularities" that led to the unauthorized over-collection of hundreds of millions of call records.

Huebner said he couldn't "go into extensive detail" on the topic, citing the pending report, but he did offer further explanation regarding one of the chief technical challenges surrounding the snooping program.

Huebner said NSA analysts noticed that telecommunications providers were giving "inaccurate" data in the early stages that irrevocably tainted the contact-chaining process that lies at the heart of the program.

"Suffice to say, some of the information coming from the providers from that first hop was inaccurate. It did not accurately indicate that phone number A was in contact with phone number B," Huebner said. "[NSA] was only authorized to receive the two-hop information, but if there was an error with that first hop, all of those additional records that came in on that second hop would be overcollection and certainly a compliance incident."

Under the program, a single order provides the NSA access to communications metadata of specific target individuals as well as anyone else up to two "hops" away. This means that in addition to the target's incoming and outgoing call records (one hop), the agency could also obtain outgoing and incoming call records for anyone who communicated with that target as well (second hop).

This meant the program was not only collecting communications metadata outside of the law, it also meant the overall value of the program was much less clear.

"If the data is inaccurate, it doesn't actually indicate an actual connection between two individuals," Huebner said. "That is not terribly useful from an intelligence perspective."

According to Huebner, it was not "immediately apparent" from the call detail records what information was accurate or inaccurate, leaving "no easy way" for NSA to sort through which records were tainted and which were not. The NSA wound up purging more than 600 million call records, and the program was shut down while Congress debates its reauthorization.

Months after it first disclosed the issue, the NSA acknowledged in a document made public by the ACLU that it still had not found a technical solution and had used some of the inaccurate information produced by the program in requests to the Foreign Intelligence Surveillance Court.

Greg Nojeim, senior counsel and director of the Freedom, Technology and Security Project at the Center for Democracy and Technology, told FCW that he was not aware of those details prior to Huebner's comments and said it likely means the NSA had "a whole slew of second-hop data that was collected illegally and that was thwarting the effort to draw intelligence value from the program."

"It appears the problem was bigger than one might have concluded based on the disclosures NSA made earlier this year," Nojeim said. "One bad call record on the first hop can generate a huge number of bad call records on the second hop, and NSA sucked them all up in violation of the law."

According to the ODNI's latest transparency report, the government pulled more than 434 million call records by targeting just 11 individuals under the program in 2018, though the agency says some of those records are duplicates.

The PCLOB report is expected to go into further detail on the technical challenges facing the program, which was originally set to expire in December but was renewed for an additional three months as part of a short-term funding measure in October. Congress will now have until March 15, 2020, to debate whether or not to reauthorize it.

While the Trump administration has requested a permanent renewal, senior leaders in Congress in both parties have signaled a desire to end the Call Detail Records once and for all, though support for other expiring Patriot Act surveillance authorities remains strong.

Huebner told FCW that declassification of the pending PCLOB report will take time and would probably be made public sometime "over the next few months." He said he was confident that it would be released before lawmakers vote on a lengthier reauthorization.