

THE UNAUDITED TECH ANALYST ACCESS TO US PERSON DATA

In addition to its exposure of the sheer senselessness of much of the spying NSA engages in, yesterday's WaPo story also shows that the government's assurances that Edward Snowden could not access raw data have been misplaced.

For close to a year, NSA and other government officials have appeared to deny, in congressional testimony and public statements, that Snowden had any access to the material.

As recently as May, shortly after he retired as NSA director, Gen. Keith Alexander denied that Snowden could have passed FISA content to journalists.

"He didn't get this data," Alexander told a New Yorker reporter. "They didn't touch —"

"The operational data?" the reporter asked.

"They didn't touch the FISA data," Alexander replied. He added, "That database, he didn't have access to."

Robert S. Litt, the general counsel for the Office of the Director of National Intelligence, said in a prepared statement that Alexander and other officials were speaking only about "raw" intelligence, the term for intercepted content that has not yet been evaluated, stamped with classification markings or minimized to mask U.S. identities.

"We have talked about the very strict controls on raw traffic, the training that people have to have, the technological lockdowns on access," Litt said. "Nothing that you have given us

indicates that Snowden was able to circumvent that in any way.”

In the interview, Snowden said he did not need to circumvent those controls, because his final position as a contractor for Booz Allen at the NSA’s Hawaii operations center gave him “unusually broad, unescorted access to raw SIGINT [signals intelligence] under a special ‘Dual Authorities’ role,” a reference to Section 702 for domestic collection and Executive Order 12333 for collection overseas. Those credentials, he said, allowed him to search stored content – and “task” new collection – without prior approval of his search terms.

No one should ever have believed those assurances.

That’s because the documentation on the Section 215 program makes it clear how little oversight there is over tech people just like Snowden. The current phone dragnet order, for example, makes it clear that:

- Tech personnel may access the phone dragnet data to tweak it in preparation for contact-chaining
- Unlike intelligence analysts, tech personnel may query the phone dragnet data with selectors that have not been RAS-approved
- Tech personnel may also conduct regular queries using RAS-approved selectors
- Tech personnel may access the dragnet data to search for high volume numbers –

this may require access to raw data

- Some of the tech personnel (those in charge of infrastructure and receiving data from the telecoms) are exempt from special training on the phone dragnet data

The audit language in the dragnet order applies only to “foreign intelligence analysis purposes or using foreign intelligence analysis tools,” suggesting the tech analysis role access to the dragnet data is not audited.

Language in the order defining “NSA” suggests contractors may access the data (though it’s unclear whether they do so in a technical or intelligence analysis function); something made explicit in Dianne Feinstein’s bill.

That is, it is at least possible that Booz analysts are currently conducting audit-free tech massaging of the raw phone dragnet data.

And NSA knew this access was a vulnerability. As recently as 2012, tech analysts were found to have 3,000 files worth of phone dragnet data (it’s unclear how much data each file included) on an improper server past its required destruction date. NSA destroyed that data before definitively researching what it was doing there.

Thus, the risk of tech analyst breach is very real, and no one – not NSA, and not Congress, which has only codified this arrangement – seems to be addressing it.

Indeed, it is likely that some kind of Booz-type contractors will continue to have direct access to this data after it gets outsourced to the telecoms, otherwise USA Freedom would not extend immunity to such second-level contractors.

For months, intelligence officials claimed not

only that Snowden had not accessed raw data, but could not. That was always a dubious claim; even if Snowden couldn't have accessed that data, other contractors just like him could and still can, with less oversight than NSA's intelligence analysts get.

But it turns out Snowden could and did. And thanks to that, we now know many of the other claims made by government witnesses are also false.