NSA'S DRAGNET FAILED TO "CORRELATE" DAVID HEADLEY'S IDENTITY, ONE OF ITS CORE FUNCTIONS

In a piece on the GCHQ and NSA failure to identify David Headley's role in the Mumbai terrorist attack, ProPublica quotes former CIA officer Charles Faddis on the value of bulk surveillance.

> "I'm not saying that the capacity to intercept the communications is not valuable," said Charles (Sam) Faddis, a former C.I.A. counterterror chief. "Clearly that's valuable." Nonetheless, he added, it is a mistake to rely heavily on bulk surveillance programs in isolation.
>
> "You're going to waste a lot of money, you're going to waste a lot of time," Faddis said. "At the end, you're going have very little to show for it."

The article as a whole demonstrates that in a manner I'm fairly shocked about. The NSA failed to recognize what it had in intelligence collected on Headley's role in the attack *even after the attack* because they hadn't correlated his *known birth name* with the name he adopted in the US.

> Headley represents another potential stream of intelligence that could have made a difference before Mumbai. He is serving 35 years in prison for his role. He was a Pakistani-American son of privilege who became a heroin addict, drug smuggler and DEA informant, then an Islamic terrorist and Pakistani spy, and finally, a prize witness for U.S.

> prosecutors.
>
> In recounting that odyssey, we previously explored half a dozen missed opportunities by U.S. law enforcement to pursue tips from Headley's associates about his terrorist activity. New reporting and analysis traces Headley's trail of suspicious electronic communications as he did reconnaissance missions under the direction of Lashkar and Pakistan's Inter-Services Intelligence Directorate (ISI).
>
> Headley discussed targets, expressed extremist sentiments and raised other red flags in often brazen emails, texts and phone calls to his handlers, one of whom worked closely on the plot with Shah, the Lashkar communications chief targeted by the British.
>
> U.S. intelligence officials disclosed to me for the first time that, after the attacks, intensified N.S.A. monitoring of Pakistan did scoop up some of Headley's suspicious emails. But analysts did not realize he was a U.S.-based terrorist involved in the Mumbai attacks who was at work on a new plot against Denmark, officials admitted.
>
> The sheer volume of data and his use of multiple email addresses and his original name, Daood Gilani, posed obstacles, U.S. intelligence officials said. To perfect his cover as an American businessman, Headley had legally changed his name in 2006.
>
> "They detected a guy named 'Gilani' writing to bad guys in Pakistan, communicating with terror and ISI nodes," a senior U.S. intelligence official said. "He wrote also in fluent Urdu, which drew interest. Linking 'Gilani' to 'Headley' took a long time. The N.S.A. was looking at those emails

> post-Mumbai. It was not clear to them who he was."

As I've explained, one of the things NSA does with all its data is to "correlate" selectors, so that it maps a picture of all the Internet and telecom (and brick and mortar, where they have HUMINT) activities of a person using the multiple identities that have become common in this day and age. This is a core function of the NSA's dragnets, and it works automatically on EO 12333 data (and worked automatically on domestically-collected phone and — probably — Internet metadata until 2009).

When you think about it, there are some easy ways of matching online identities (going to a provider, mapping some IP addresses). And even the matching of "burner" IDs can be done with 94% accuracy, at least within AT&T's system, according to AT&T's own claims.

The NSA says they didn't do so here because Headley had changed his name.

Headley, recall, was a DEA informant. Which means, unless these intelligence agencies are far more incompetent than I believe they are, this information was sitting in a government file somewhere: "Daood Gilani, the name of a known Urdu-fluent informant DEA sent off to Pakistan to hang out with baddies = David Headley." Unless Headley adopted the new name precisely because he knew it would serve to throw the IC off his trail.

And yet … NSA claims it could not, and did not, correlate those two identities and as a result didn't even realize Headley was involved in the Mumbai bombing even after the attack.

Notably, they claim they did not do so because of the "sheer volume of data."

In short, according to the NSA's now operative story (you should click through to read the flaccid apologies the IC offered up for lying about the value of Sections 215 and 702 in

catching Headley), the NSA’s dragnet failed at one of its core functions because it is drowning in data.