

THE HEROIC IRS AGENT STORY SHOULD RAISE MORE QUESTIONS ABOUT SILK ROAD INVESTIGATION

“In these technical investigations, people think they are too good to do the stupid old-school stuff. But I’m like, ‘Well, that stuff still works.’ ”

The NYT got this and many other direct quotes from IRS agent Gary Alford for a complimentary profile of him that ran on Christmas day. According to the story, Alford IDed Ross Ulbricht as a possible suspect for the Dread Pirate Roberts – the operator of the Dark Web site Silk Road – in early June 2013, but it took until September for Alford to get the prosecutor and DEA and FBI Agents working the case to listen to him. The profile claims Alford’s tip was “crucial,” though a typo suggests NYT editors couldn’t decide whether it was *the* crucial tip or just crucial.

In his case, though, the information he had was the crucial [sic] to solving one of the most vexing criminal cases of the last few years.

On its face, the story (and Alford’s quote) suggests the FBI is so entranced with its hacking ability that it has neglected very, very basic investigative approaches like Google searches. Indeed, if the story is true, it serves as proof that encryption and anonymity don’t thwart FBI investigations as much as Jim Comey would like us to believe when he argues the Bureau needs to back door all our communications.

But I don’t think the story tells the complete

truth about the Silk Road investigation. I say that, first of all, because of the timing of Alford's efforts to get others to further investigate Ulbricht. As noted, the story describes Alford IDing Ulbricht as a potential suspect in early June 2013, after which he put Ulbricht's name in a DEA database of potential suspects, which presumably should have alerted anyone else on the team that US citizen Ross Ulbricht was a potential suspect in the investigation.

Mr. Alford's preferred tool was Google. He used the advanced search option to look for material posted within specific date ranges. That brought him, during the last weekend of May 2013, to a chat room posting made just before Silk Road had gone online, in early 2011, by someone with the screen name "altoid."

"Has anyone seen Silk Road yet?" altoid asked. "It's kind of like an anonymous Amazon.com."

The early date of the posting suggested that altoid might have inside knowledge about Silk Road.

During the first weekend of June 2013, Mr. Alford went through everything altoid had written, the online equivalent of sifting through trash cans near the scene of a crime. Mr. Alford eventually turned up a message that altoid had apparently deleted – but that had been preserved in the response of another user.

In that post, altoid asked for some programming help and gave his email address: rossulbricht@gmail.com. Doing a Google search for Ross Ulbricht, Mr. Alford found a young man from Texas who, just like Dread Pirate Roberts, admired the free-market economist Ludwig von Mises and the libertarian politician Ron Paul – the first of many striking

parallels Mr. Alford discovered that weekend.

When Mr. Alford took his findings to his supervisors and failed to generate any interest, he initially assumed that other agents had already found Mr. Ulbricht and ruled him out.

But he continued accumulating evidence, which emboldened Mr. Alford to put Mr. Ulbricht's name on the D.E.A. database of potential suspects, next to the aliases altoid and Dread Pirate Roberts.

At the same time, though, Mr. Alford realized that he was not being told by the prosecutors about other significant developments in the case – a reminder, to Mr. Alford, of the lower status that the I.R.S. had in the eyes of other agencies. And when Mr. Alford tried to get more resources to track down Mr. Ulbricht, he wasn't able to get the surveillance and the subpoenas he wanted.

Alford went to the FBI and DOJ with Ulbricht's ID in June 2013, but FBI and DOJ refused to issue even subpoenas, much less surveil Ulbricht.

But over the subsequent months, Alford continued to investigate. In "early September" he had a colleague do another search on Ulbricht, which revealed he had been interviewed by Homeland Security in July 2013 for obtaining fake IDs.

In early September, he asked a colleague to run another background check on Mr. Ulbricht, in case he had missed something.

The colleague typed in the name and immediately looked up from her computer: "Hey, there is a case on this guy from July."

Agents with Homeland Security had seized

a package with nine fake IDs at the Canadian border, addressed to Mr. Ulbricht's apartment in San Francisco. When the agents visited the apartment in mid-July, Mr. Ulbricht answered the door, and the agents identified him as the face on the IDs, without having any idea of his potential links to Silk Road.

When Alford told prosecutor Serrin Turner of the connection (again, this is September 2013), the AUSA finally did his own search in yet another database, the story claims, only to discover Ulbricht lived in the immediate vicinity of where Dread Pirate Roberts was accessing Silk Road. And that led the Feds to bust Ulbricht.

I find the story – the claim that without Alford's Google searches, FBI *did not* and would not have IDed Ulbricht – suspect for two reasons.

First, early June is the date that FBI Agent Christopher Tarbell's declaration showed (but did not claim) FBI first hacked Silk Road. That early June date was itself suspect because Tarbell's declaration really showed data from as early as February 2013 (which is, incidentally, when Alford was first assigned to the team). In other words, while it still seems likely FBI was always lying about when it hacked into Silk Road, the coincidence between when Alford says he went to DOJ and the FBI with Ulbricht's ID and when the evidence they were willing to share with the defense claimed to have first gotten a lead on Silk Road is of interest. All the more so given that the FBI claimed it could legally hack the server because it did not yet know the server was run by an American, and so it treated the Iceland-based server as a foreigner for surveillance purposes.

One thing that means is that DOJ may not have wanted to file paperwork to surveil Ulbricht because admitting they had probable cause to suspect an American was running Silk Road would

make their hack illegal (and/or would have required FBI to start treating Ulbricht as the primary target of the investigation; it seems FBI may have been trying to do something else with this investigation). By delaying the time when DOJ took notice of the fact that Silk Road was run by an American, they could continue to squat on Silk Road without explaining to a judge what they were doing there.

The other reason I find this so interesting is because several of the actions to which corrupt DEA agent Carl Force pled guilty – selling fake IDs and providing inside information – took place between June and September 2013, during the precise period when everyone was ignoring Alford's evidence *and* the fact that he had entered Ulbricht's name as a possible alias for the Dread Pirate Roberts into a DEA database. Of particular note, Force's guilty plea only admitted to selling the fake IDs for 400 bitcoin, and provided comparatively few details about that action, but the original complaint against Force explained he had sold the IDs for 800 bitcoin but refunded Ulbricht 400 bitcoin because "the deal for the fraudulent identification documents *allegedly* fell through" [emphasis mine].

Were those fake IDs that Force sold Ulbricht the ones seized by Homeland Security and investigated in July 2013? Did the complaint say the deal "allegedly" fell through because it didn't so much fall through as get thwarted? Did something – perhaps actions by Force – prevent other team members from tying that seizure to Ulbricht? Or did everyone know about it, but pretend not to, until Alford made them pay attention (perhaps with a communications trail that other Feds couldn't suppress)? Was the ID sale part of the investigation, meant to ID Ulbricht's identity and location, but Force covered it up?

In other words, given the record of Force's actions, it seems more likely that at least some people on the investigative team already knew

what Alford found in a Google search, but for both investigative (the illegal hack that FBI might have wanted to extend for other investigative reasons) and criminal (the money Force was making) reasons, no one wanted to admit that fact.

Now, I'm not questioning the truth of what Alford told the NYT. But even his story (which is corroborated by people "briefed on the investigation," but only one person who actually attended any of the meetings for it; most of *those* people are silent about Alford's claims) suggests there may be other explanations why no one acted on his tip, particularly given the fact that he appears to have been unable to do database searches himself and that they refused to do further investigation into Ulbricht. (I also wonder whether Alford's role explains why the government had the IRS in San Francisco investigate Force and corrupt Secret Service Agent Shaun Bridges, rather than New York, where agents would have known these details.)

Indeed, I actually think this complimentary profile might have been a way for Alford to expose further cover-ups in the Silk Road investigation without seeming to do so for any but self-interested reasons. Bridges was sentenced on December 7. Ulbricht was originally supposed to have submitted his opening appellate brief – focusing on Fourth Amendment issues that may be implicated by these details – on December 11, but on December 2, the court extended that deadline until January 12.

I don't know whether Ulbricht's defense learned these details. I'm admittedly not familiar enough with the public record to know, though given the emphasis on Tarbell's declaration as the explanation for how they discovered Ulbricht and the NYT's assertion Alford's role and the delay was "largely left out of the documents and proceedings that led to Mr. Ulbricht's conviction and life sentence this year," I don't think it is public. But if they didn't, then the

fact that the investigative team went out of their way to avoid confirming Ulbricht's readily accessible identity until at least three and probably seven months after they started hacking Silk Road, even while key team members were stealing money from the investigation, might provide important new details about the government's actions.

And if Alford gets delayed credit for doing simple Google searches as a result, all the better!