CORRELATIONS AND FBI CLAIMS IN THE MARATHON TRIAL

Kevin Swindon, the FBI Supervisory Special Agent in charge of computer forensics for the Boston Marathon attack just finished testimony. His testimony raised more questions than it answered. That's true, in part, because the government had him testify rather than some of the Agents who report to him who did the actual analysis on the many devices related to the investigation. So for key questions, he had to answer he didn't know. He also dodged explaining who cherry picked the files to present to the jury that made Dzhokhar Tsarnaev look singularly focused on jihad when his computer showed he was more interested in pop music and something else — probably sexual? — that young men are often interested in.

On cross, Dzhokhar's attorney William Fick tried to direct Swindon to describe more about a laptop found at Watertown that apparently belonged to Tamerlan. Swindon admitted the laptop — unlike all the computers Dzhokhar used — used strong encryption and also had a goodly number of Russian language documents on explosives. But over and over Swindon claimed he had only taken a "cursory" look at that computer.

I'm betting the person who did the more than cursory analysis of it would be a far more interesting witness and that's why we didn't hear from him or her. Not only will we not get to hear from that witness, apparently, but Judge George O'Toole upheld a prosecution objection to ask further questions about it.

Before that, prosecutor Aloke Chakravarty led Swindon through a very bizarre exercise. He had Swindon show how the same songs that were one one of Dzhokhar's devices showed up on another. He showed continuity between an iPod, a Samsung

phone, and the Sony found at his dorm room. In other words, the government used common songs as a means to correlate these computers, rather than actual forensic evidence that Swindon surely could have presented. I find that really problematic. Sure, the government probably wants to pretend it doesn't do such correlations forensically, but to suggest that someone's musical downloads shows common ownership seems really problematic.

All the more so given that for another of the computers (I'm not sure if this is Dzhokhar's college computer or the HP at Tsarnaev house in Cambridge, but it may not matter as Dzhokhar's computer dated to when he still lived at home) there was evidence of multiple Skype users, though Swindon claimed to be unaware of that fact. We know the government correlates using such things, and the fact that evidence of others users was deliberately not presented (probably through choice of witness more than through deceit) is really problematic.

The defense also showed that the thumb drive found in the computer that Dzhokhar's buddies had thrown out had a rental application from his sister-in-law, showing that whether or not he used these devices in common, plenty of other people were using them as well.

In short, the government wanted to use really problematic correlations mapping to prove that Dzhokhar was accessing jihadist material (even though a question about whether one of the computers had ever searched on the term was not permitted), but they can't even prove who was using any of the computers when, and pointedly avoided using real forensics means to do so.