WILLIAM WEBSTER MEETS EDWARD SNOWDEN, IRTPA, ROVING WIRETAPS, AND THE PHONE DRAGNET

For a post on back-door searches, I'm re-reading the William Webster report on whether the FBI could have anticipated Nidal Hasan's attack. In the light of the Edward Snowden disclosure, I'm finding there are a number of passages that read very differently (so expect this to be a series of posts).

As you read this, remember two things about Webster's report. First, FBI and NSA's failure to find Umar Farouk Abdulmutallab in spite of texts he sent to Anwar al-Awlaki was probably prominent on the Webster team's mind as they completed this (and surely factors significantly in the classified version of the SSCI report on the UndieBomb). So some of the comments in the Webster report probably don't apply directly to the circumstances of Nidal Hasan, but to that (and Webster notes that some of the topics he addresses he does because they're central to counterterrorism approaches). And the Webster report is perhaps the most masterful example of an unclassified document that hides highly classified background.

All that said, in a section immediately following Webster's description of Section 215, Webster discusses how Roving Wiretaps, Section 6001 of IRTPA, and Section 215 were all reauthorized in 2011.

> When FISA was passed in 1978, the likely targets of counterterrorism surveillance were agents of an organized terrorist group like the Red Brigades, the Irish Republican Army, or the Palestinian terrorist organizations of that era.

> **Given the increasing fluidity in the membership and organization of international terrorists**, the FBI may not be able to ascertain a foreign terrorist's affiliation with an international organization. Section 6001 of the Intelligence Reform and Terrorist Prevention Act of 2004 (IRTPA) allows the government to conduct surveillance on a non-U.S. person who "engages in international terrorism or activities in preparation therefor" without demonstrating an affiliation to a particular international terrorist organization. Pub. L. 108-458, § 6001, 118 Stat. 3638, 3742 (2004).
>
> Sections 206 and 215 of the PATRIOT Act and Section 6001 of IRTPA were scheduled to "sunset" on December 31, 2009. In May 2011, after an interim extension, Congress extended the provisions until June 1, 2015, without amendment. [my emphasis]

I find this interesting, first of all, because it doesn't mention the Pen Register and Lone Wolf language that also got reauthorized in 2011 (suggesting he lumped these three together for a specific reason). And because it puts the language, "engages in international terrorism or activities in preparation therefor" together with roving wiretaps ("continuous electronic surveillance as a target moves from one device to another"), and Section 215, which we now know includes the phone dragnet.

As we've seen, DiFi's Fake FISA Fix includes the language from IRTPA, on "preparation therefor," which I thought was an expansion of potential targets but which I presume now is what they've been using all along. While I don't recall either the White Paper nor Claire Eagan's language using that language, I'm wondering whether some underlying opinion does.

Now consider how the roving wiretap goes with

this. One reason — probably the biggest reason — they need all phone records in the US is so they can use it to find targets as they move from one burner cell phone to another. Indeed, one passage from DiFi's Fake FISA Fix seems specifically designed to authorize this kind of search.

> (C) to or from any selector reasonably linked to the selector used to perform the query, in accordance with the court approved minimization procedures required under subsection (g).

That language "reasonably linked" surely invokes the process of using algorithms to match calling patterns to calling patterns to find a target's new phone. And note this is the only query that mentions minimization procedures, so the Court must have imposed certain rules about how you treat a new "burner" phone ID until such time as you've proven it actually is linked to the first one.

What's interesting, though, is that the Webster report also lumps roving wiretaps in with this. What's at issue in Nidal Hasan's case was effectively roving electronic communication; he emailed Awlaki from several different email addresses and one of the problems FBI had was in pulling up Hasan's communications under both identities (you can see how this relates to the back door loophole). But the inclusion of roving wiretaps here seems to suggest the possibility that a court has used the existing of roving wiretap approval for the use of the phone dragnet to find burner phones (which shouldn't have been an issue in the Nidal Hasan case but probably was for Abdulmutallab).

One more comment? The notion that identifying an Al Qaeda target is any harder than identifying an IRA-affiliate is utter nonsense. If anything, US-based IRA affiliates were harder to identify because they were completely and utterly socially acceptable. But I guess such myths are important for people advocating more dragnet.