THE 2011 DIOG PERMITS USING NSLS TO GET JOURNALIST CONTACTS

In what may be one of those stories telegraphing investigative details between people being investigated, the WaPo updates the StuxNet investigation.

> Prosecutors are pursuing "everybody — at pretty high levels, too," said one person familiar with the investigation. "There are many people who've been contacted from different agencies."
>
> The FBI and prosecutors have interviewed several current and former senior government officials in connection with the disclosures, sometimes confronting them with evidence of contact with journalists, according to people familiar with the probe.

Here's the detail everyone is focusing on (and I've seen similar claims on reporting of other leak investigations).

> Investigators, they said, have conducted extensive analysis of the e-mail accounts and phone records of current and former government officials in a search for links to journalists.
>
> [snip]
>
> Former prosecutors said these investigations typically begin by compiling a list of people with access to the classified information. When government officials attend classified briefings or examine classified documents in secure facilities, they must sign a log, and these records can provide an initial road map for investigators.

> **Former prosecutors** said investigators run sophisticated software to identify names, key words and phrases embedded in e-mails and other communications, including text messages, which could lead them to suspects.
>
> The FBI also looks at officials' phone records — who called whom, when, for how long. Once they have evidence of contact between officials and a particular journalist, investigators can seek a warrant to examine private e-mail accounts and phone records, including text messages, former prosecutors said.
>
> Prosecutors and the FBI can examine government e-mail accounts and government-issued devices, including cellphones, without a warrant. They can also look at private e-mail accounts without a warrant if those accounts were accessed on government computers. [my emphasis]

This description may well be how the government is conducting the StuxNet (and the UndieBomb 2.0 investigation, which the article also describes).

But if WaPo is relying solely on **former** prosecutors, this description may be totally outdated.

After all—as I've reported repeatedly in the past—the 2011 update of FBI's Domestic Investigations and Operations Guide permits using National Security Letters to get journalists' contacts in National Security investigations (as all of these would be).

> A heavily-redacted section (PDF 166) suggests that in investigations with a national security nexus (so international terrorism or espionage, as many leak cases have been treated) DOJ need not comply with existing restrictions requiring Attorney General

> approval before getting the phone records of a journalist. The reason? Because NSLs aren't subpoenas, and that restriction only applies to subpoenas.
>
> > Department of Justice policy with regard to the issuances of subpoenas for telephone toll records of members of the news media is found at 28 C.F.R. § 50.10. **The regulation concerns only grand jury subpoenas, not National Security Letters (NSLs) or administrative subpoenas**. (The regulation requires Attorney General approval prior to the issuance of a grand jury subpoena for telephone toll records of a member of the news media, and when such a subpoena is issued, notice must be given to the news media either before or soon after such records are obtained.) The following approval requirements and specific procedures apply for the issuance of an NSL for telephone toll records of members of the news media or news organizations. [my emphasis]
>
> So DOJ can use NSLs—with no court oversight—to get journalists' call (and email) records rather than actually getting a subpoena.
>
> The section includes four different approval requirement scenarios for issuing such NSLs, almost all of which are redacted. Though one only partly redacted passage makes it clear there are some circumstances where the approval process is the same as for anyone else DOJ wants to get an NSL on:
>
> > If the NSL is seeking telephone

> toll records of an individual who is a member of the news media or news organization [2 lines redacted] there are no additional approval requirements other than those set out in DIOG Section 18.6.6.1.3 [half line redacted]

And the section on NSL use (see PDF 100) makes it clear that a long list of people can approve such NSLs:

- *Deputy Director*
- *Executive Assistant Director*
- *Associate EAD for the National Security Branch*
- *Assistant Directors and all DADs for CT/CD/Cyber*
- *General Counsel*
- *Deputy General Counsel for the National Security Law Branch*
- *Assistant Directors in Charge in NY, Washington Field Office, and LA*
- *All Special Agents in Charge*

In other words, while DOJ does seem to offer members of the news media—which is itself a somewhat limited group—some protection from subpoena, it also seems to include loopholes for precisely the kinds of cases, like leaks, where source protection is so important.

In other words, this story about starting with the sign-in logs of people who've been briefed on a particular topic, then gather call records of those officials?

That may be what happened.

Or it may work the other way, with the government identifying a story it doesn't like and then using call records to trace back from there to the potential sources of the story.

This curious phrasing would support the latter scenario.

> [DC US Attorney Ronald] Machen is examining a leak to the Associated Press that a double agent inside al-Qaeda's affiliate in Yemen allowed the United States and Saudi Arabia to disrupt the plot to bomb an airliner using explosives and a detonation system that could evade airport security checks.

The AP, after all, didn't report that UndieBomb 2.0 was actually a sting set up by a Saudi-run infiltrator (and their reporting, at least, suggested they didn't know UndieBomber 2.0 was an informant). John Brennan and Richard Clarke told that story. And yet WaPo describes the investigation as focusing on the AP part of the story, not the more damning part about an infiltrator.

If and when John Brennan goes unpunished for revealing the most damning part of this story, it'll become increasingly clear: not only is the government starting with the journalists' phone and email contacts, but it is doing so with journalists it might otherwise want to silence.