DOJ'S REAFFIRMATION OF JOURNALIST NSLS AND THE UNDIEBOMB 2.0 AND STUXNET INVESTIGATIONS

Given Friday's news that DOJ's "new" media guidelines continue to permit FBI to use National Security Letters to obtain journalists' contact information, I'd like to return to the apparent results of two major leak investigations, those into the UndieBomb 2.0 and StuxNet leaks.

In the former case, the DOJ claims it had no idea that Donald Sachtleben served as a source for Matt Apuzzo and Adam Goldman's story on UndieBomb 2.0 and no means to get a warrant for a computer they already had in their possession until — months into the investigation — they subpoenaed the phone records for 20 AP lines.

> The entire premise of the FBI narrative is that they exercised greater care with a kiddie porn accusee they had dead to rights than they did the 100 or so AP reporters who got sucked up in their overbroad dragnet. They would have you believe that, even after seizing a CD holding a November 2, 2006 SECRET CIA intelligence report at Sachtleben's house in May 2012 pursuant to a kiddie porn warrant (which they have not produced in the docket), they just sat on his devicesfor almost a year until they obtained the phone records for 20 AP phone lines, in a seizure far more intrusive into journalism than any recent known subpoena.
>
> > Sachtleben was identified as a suspect in the case of this unauthorized disclosure only

> > after toll records for phone numbers related to the reporter were obtained through a subpoena and compared to other evidence collected during the leak investigation. This allowed investigators to obtain a search warrant authorizing a more exhaustive search of Sachtleben's cell phone, computer, and other electronic media, which were in the possession of federal investigators due to the child pornography investigation.
>
> (I may be mistaken, but I don't think the FBI made this claim in any court document, so I assume it is bullshit, especially since they had had to do extensive forensic searches of Sachtleben's computer and he had already signed a plea deal forfeiting it.)

In addition, DOJ would have you believe that Sachtleben, who could not have been the most important source for this leak, was the AP's only source. At his sentencing, he pointed out correctly that's not true.

> "I was neither the sole nor the original source of information to 'Reporter A' about the suicide bomb," Sachtleben said in a statement sent by his law firm. "The information I shared with Reporter A merely confirmed what he already believed to be true. Any implication that I was the direct source of a serious leak is an exaggeration."

And the transcript of John Brennan's teleconference to guide this leak makes it clear that the AP had far more information than they published, Sachtleben leaks all appeared in the story. So there obviously were far more

sensitive sources DOJ chose not to prosecute.

They got their kiddie porn scapegoat, and their public explanation of how and why they obtained the phone records implicating 100 AP journalists. Which presumably had the additional advantage of making it clear to all Apuzzo and Goldman's potential sources that DOJ is willing to go after them.

Compare all that to the StuxNet investigation. Reports last year identified Retired General James Cartwright as the suspect in the case.

> But, said legal sources, while the probe that Attorney General Eric Holder ordered initially focused on whether the information came from inside the White House, by late last year FBI agents were zeroing in on Cartwright, who had served as one of the president's "inner circle" of national security advisors.

The investigation focused on Cartwright in spite of evidence the White House was closely involved in the book (though not necessarily involved in leaking the details that particularly angered DC insiders, which may have been the that Israel permitted the virus to escape).

And all this happened — FBI was able to rule out the White House's sources but still confirm Cartwright's role — without subpoenaing NYT phone records.

> Two sources said prosecutors were able to identify Cartwright as a suspected leaker without resorting to a secret subpoena of the phone records of New York Times reporters.

As it happens, Cartwright was only stripped of his clearance, not charged; there will be no court case in which the government has to show how it collected its evidence against Cartwright.

Of course, it would be a lot easier to pick and

choose which sources to prosecute if you can secretly identify, using National Security Letters, those sources before actually obtaining journalist records in a way that requires public notice, as the AP subpoena eventually did. And then, at such time as you do want to make that public, you can get the subpoena showing the evidence you've already obtained via NSL.

In addition to being a threat to press freedoms, the explicit use of NSLs to obtain journalist contacts permits the government even more arbitrary power than the record of these two cases show it exercises.

Using NSLs allows DOJ to engage in selective leak prosecutions without that being immediately obvious.

Handy things, these NSLs.