THE TWO OLC STILL-SECRET MEMOS BEHIND THE CROSS-BORDER KEYWORD SEARCHES?

Last week, Charlie Savage explained what this paragraph from the NSA's targeting document means.

> In addition, in those cases where NSA seeks to acquire communications about the target that are not to or from the target, SNA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or it will target Internet links that terminate in a foreign country. In either event, NSA will direct surveillance at a party to the communication reasonably believed to be outside the United States.

Savage explained that it refers to the way the US snoops through almost all cross-border traffic for certain keywords.

> To conduct the surveillance, the N.S.A. is temporarily copying and then sifting through the contents of what is apparently most e-mails and other text-based communications that cross the border. The senior intelligence official, who, like other former and current government officials, spoke on condition of anonymity because of the sensitivity of the topic, said the N.S.A. makes a "clone of selected communication links" to gather the communications, but declined to specify details, like the volume of the data that passes through them.
>
> [snip]

> The official said that a computer searches the data for the identifying keywords or other “selectors” and stores those that match so that human analysts could later examine them. The remaining communications, the official said, are deleted; the entire process takes “a small number of seconds,” and the system has no ability to perform “retrospective searching.”
>
> The official said the keyword and other terms were “very precise” to minimize the number of innocent American communications that were flagged by the program. At the same time, the official acknowledged that there had been times when changes by telecommunications providers or in the technology had led to inadvertent overcollection. The N.S.A. monitors for these problems, fixes them and reports such incidents to its overseers in the government, the official said.

In his post on Savage’s story (which I think misreads what Savage describes), Ben Wittes focused closely on the last paragraphs of the story.

> But that leaves a big oddity with respect to the story. The end of Savage’s story reads as follows:
>
> > There has been no public disclosure of any ruling by the Foreign Intelligence Surveillance Court explaining its legal analysis of the 2008 FISA law and the Fourth Amendment as allowing “about the target” searches of Americans’ cross-border communications. But in 2009, the Justice Department’s Office of Legal Counsel signed off on a similar process for searching federal

> > employees' communications without a warrant to make sure none contain malicious computer code.
>
> That opinion, by Steven G. Bradbury, who led the office in the Bush administration, may echo the still-secret legal analysis. He wrote that because that system, called EINSTEIN 2.0, scanned communications traffic "only for particular malicious computer code" and there was no authorization to acquire the content for unrelated purposes, it "imposes, at worst, a minimal burden upon legitimate privacy rights."

The Bradbury opinion was echoed by a later Obama-era opinion by David Barron, and Bradbury later wrote an article about the issue. But here's the thing: If my read is right and the rule Savage cites permits only acquisition of communications "about" potential targets only from folks reasonably believed themselves to be overseas, these opinions are of questionable relevance. Indeed, if my reading is correct, why is there a Fourth Amendment issue here at all? The Fourth Amendment, after all, does not generally have extraterritorial application. This may be a reason to suspect that the issue is more complicated than I'm suggesting here. It may also merely suggest that someone cited to Savage a memo that is of questionable relevance to the issue at hand.

In his letter to John Brennan in January asking for a slew of things, Ron Wyden mentioned two opinions that may be the still-secret legal analysis mentioned by Savage.

> Third, over two years ago, Senator Feingold and I wrote to the Attorney General regarding two classified opinions from the Justice Department's Office of Legal Counsel, including an opinion that interprets common commercial service agreements. We asked the Attorney General to declassify both of these opinions, and to revoke the opinion pertaining to commercial service agreements. Last summer, I repeated the request, and noted that the opinion regarding commercial service agreements has direct relevance to ongoing congressional debates regarding cybersecurity legislation. The Justice Department still has not responded to these letters.

The opinions would have to pre-date January 14, 2011, because Feingold and Wyden requested the opinions before that date.

The reason I think the service agreements one may be relevant is because the opinions Ben cites focus on whether government users have given consent for EINSTEIN surveillance; in his article on it Bradbury focuses on whether the government could accomplish something similar with critical infrastructure networks.

Remember, we do know of one OLC memo — dated January 8, 2010 — that pertains to the government obtaining international communications willingly from service providers. We learned about it in the context of the Exigent Letters IG Report, which first led observers to believe it pertained to phone records.

But we've subsequently learned this is the passage of ECPA the OLC interpreted creatively in secret.

> (f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of

> 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.

Savage's reference to the Bradbury opinion suggests all this happens at the packet stage, which may be one (arguably indefensible) way around the electronic communications dodge.

The FBI had not relied on the opinion as of 2010, when we first learned about it. But we also know that since then, the government stopped collecting Internet metadata using a Pen Regsiter/Trap and Trace order.

We know that Feingold and Wyden, with Dick Durbin, asked for a copy of the opinion themselves shortly after the IG Report revealed it. It's possible that the former two asked for it to be declassified.

This is, frankly, all a wildarsed guess. But Wyden certainly thinks there are two problematic OLC memos out there pertaining to cybersecurity. And Savage seems to think this process parallels the means the government is using for cybersecurity. So it may be these are the opinions.