JUDGE WHITE MAKES CRUCIAL ERROR WHILE CAPITULATING TO STATE SECRETS, AGAIN

Judge Jeffrey White, who has been presiding over the EFF's challenges to warrantless wiretapping since Vaughn Walker retired, just threw out part of Carolyn Jewel's challenge to the dragnet on standing and state secrets ground (h/t Mike Scarcella).

> Based on the public record, the Court finds that the Plaintiffs have failed to establish a sufficient factual basis to find they have standing to sue under the Fourth Amendment regarding the possible interception of their Internet communications. Further, having reviewed the Government Defendants' classified submissions, the Court finds that the Claim must be dismissed because even if Plaintiffs could establish standing, a potential Fourth Amendment Claim would have to be dismissed on the basis that any possible defenses would require impermissible disclosure of state secret information.

White also does what no self-respecting judge should ever do: cite Sammy Alito on Amnesty's "speculative" claims about Section 702 collection in Amnesty v. Clapper, which have since been proven to be based off false government claims.

> In Clapper, the Court found that allegations that plaintiffs' communications were intercepted were too speculative, attenuated, and indirect to establish injury in fact that was fairly traceable to the governmental surveillance activities. Id. at 1147-50.

> The Clapper Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to establish a "certainly impending" injury.

Also along the way, White claims the plaintiffs had made errors in their depiction of the upstream dragnet.

But I'm fairly certain he has done the same when he claims that only specific communications accounts can be targeted under both PRISM and upstream Section 702 collection.

> Once designated by the NSA as a target, the NSA tries to identify a specific means by which the target communicates, such as an e-mail address or telephone number. That identifier is referred to a "selector." Selectors are only specific communications accounts, addresses, or identifiers. (See id; see also Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Report") at 32-33, 36.)

Indeed, his citation to PCLOB doesn't support his point at all. Here are what I guess he means to be the relevant sections.

> The Section 702 certifications permit non-U.S. persons to be targeted only through the "tasking" of what are called "selectors." A selector must be a specific communications facility that is assessed to be used by the target, such as the target's email address or telephone number.113 Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be

> located outside the United States) are targeted; selectors (e.g., email addresses, telephone numbers) are tasked.
>
> [snip]
>
> Because such terms would not identify specific communications facilities, selectors may not be key words (such as "bomb" or "attack"), or the names of targeted individuals ("Osama Bin Laden").114 Under the NSA targeting procedures, if a U.S. person or a person located in the United States is determined to be a user of a selector, that selector may not be tasked to Section 702 acquisition or must be promptly detasked if the selector has already been tasked.115
>
> [snip]
>
> The process of tasking selectors to acquire Internet transactions is similar to tasking selectors to PRISM and upstream telephony acquisition, but the actual acquisition is substantially different. Like PRISM and upstream telephony acquisition, the NSA may only target non-U.S. persons by tasking specific selectors to upstream Internet transaction collection.131 And, like other forms of Section 702 collection, selectors tasked for upstream Internet transaction collection must be specific selectors (such as an email address), and may not be key words or the names of targeted individuals.132

First of all, unless they've changed the meaning of "such as" and "for example," PCLOB's use of email and telephone numbers is not exhaustive (though it does mirror the party line witnesses before PCLOB used, and accurately reflects PCLOB's irresponsible silence on the use of 702 — upstream and downstream — for cybersecurity,

even after ODNI has written publicly on the topic). Indeed, the NSA uses other selectors, including cyberattack signatures, in addition to things more traditionally considered a selector.

And given the government's past, documented, expansion of the term "facility" beyond all meaning, there's no reason to believe the government's use of "use" distinguishes appropriately between participants in communications.

Ah well, all that discussion probably counts as a state secret. A concept which is getting more and more farcical every year.

Update: Clarified to note this is only partial summary judgment.