WHY WOULD YOU SEGREGATE THE FISA ORDERS, BUT NOT THE DIRECTIVES?

The FBI, according to Eli Lake, thinks someone besides Edward Snowden may be responsible for leaking the Section 215 order to Verizon ordering them to turn over the metadata on all their American customers' calls. They claim to think so because digital copies of such orders exist in only two places: computers at the FISA Court and FBI's National Security Division that are segregated from the Internet. (Note: where Lake says "warrant" in this passage, he means "order.")

> Those who receive the warrant—the first of its kind to be publicly disclosed—are not allowed "to disclose to any other person" except to carry out its terms or receive legal advice about it, and any person seeing it for those reasons is also legally bound not to disclose the order. The officials say phone companies like Verizon are not allowed to store a digital copy of the warrant, and that the documents are not accessible on most NSA internal classified computer networks or on the Joint Worldwide Intelligence Communications System, the top-secret internet used by the U.S. intelligence community.
>
> The warrants reside on two computer systems affiliated with the Foreign Intelligence Surveillance Court and the National Security Division of the Department of Justice. Both systems are physically separated from other government-wide computer networks and employ sophisticated encryption technology, the officials said. Even lawmakers and staff lawyers on the House

> and Senate intelligence committees can only view the warrants in the presence of Justice Department attorneys, and are prohibited from taking notes on the documents.

Now, when the order first leaked, I actually suspected the leaker might be in this general vicinity. If that's right, then I also suspect the FBI is interested in finding this person because he or she would be reacting to the FBI's own wrong-doing on another matter. Heck, the FBI could conduct a manhunt in this general vicinity just for fun to make sure their own wrong-doing doesn't get exposed.

Such is the beauty of secret counterintelligence investigations.

That said, Lake's reporting is an example of something I suggested in the first day of this leak: we're going to learn more about how the NSA works from leaks about the investigation of it than from the leaks themselves.

And this story provides a lot of evidence that the government guards its generalized surveillance plans more jealously than it guards it particularized surveillance targets. (See this post for a description of the difference between orders and directives specifying targets.)

Consider what kinds of documents the FISA Court produces:

- Standing Section 215 orders such as the Verizon one in question
- Particularized Section 215 orders; an example might be an order for credit card companies and Big Box stores to turn over details on all purchases of pressure

cookers in the country

- FISA Amendments Act orders generally mapping out the FAA collection (we don't know how detailed they are; they might describe collection programs at the "al Qaeda" and "Chinese hacker" level, or might be slightly more specific, but are necessarily pretty general)
- Particularized FISA warrants, targeted at individual US persons (though most of this spying, Marc Ambinder and others have claimed, is conducted by the FBI under Title III)

Aside from those particularized warrants naming US persons, FISA Court doesn't, however, produce (or even oversee) lists of the great bulk of people who are being spied on. Those are the directives NSA analysts draw up on their own, without court supervision. Those directives presumably have to be shared with the service providers in some form, though all the reporting on it suggests they don't see much of it. But, Lake's remainder that Google's list of surveillance targets had been hacked by China to identify which of its agents in the US we had identified and were surveilling makes it clear they do get the list in some form.

> In April, CIO.com quoted Microsoft's Dave Aucsmith, the senior director of the company's Institute for Advanced Technology in Governments, saying a 2009 hack of major U.S. Internet companies was a Chinese plot to learn the targets of email and

> electronic surveillance by the U.S. government. In May, the *Washington Post* reported Chinese hackers had accessed a Google database that gave it access to years' worth of federal U.S. surveillance records of counter-intelligence targets.

But the prior hack makes obvious something that has been apparent since the Verizon order leaked: China doesn't have much use for information that shows NSA is compiling a database of all calls made in the US. It does, however, have a great use for the list of its spies we've identified.

What this report seems to suggest, among other things (including that the Congressional committees don't have enough scrutiny over these orders because they're not allowed to keep their own copy of them), is that details on the particularized spying is more widely dispersed, **in part because it has to be**. Someone's got to implement that particularized spying, after all, and that requires communication that traverses multiple servers.

But the generalized stuff — the stuff the FISA Court actually oversees — is locked up in a vault like the family jewels.

You might ask yourself why the government would go to greater lengths to lock up the generalized stuff — the stuff that makes it clear the government is spying on Americans — and not the particularized stuff that has far more value for our adversaries.

Update: After the hearing today, Keith Alexander said Snowden is the source of the order, and he got it during training at Fort Meade.

> Alexander told reporters after a House Intelligence Committee hearing that the man who's acknowledged being the source of the recent leaks, Booz Allen Hamilton information technology specialist Edward Snowden, had access to the Foreign

> Intelligence Surveillance Court order and related materials during an orientation at NSA.
>
> "The FISA warrant was on a web server that he had access to as an analyst coming into the Threat Operations Center," Alexander said. "It was in a special classified section that as he was getting his training he went to."

Which suggests the leaking about someone in the FISA Court may, as I thought, be an effort to impugn people in the vicinity of the court the FBI would like to shut up.