SPCMA: THE OTHER NSA DRAGNET SUCKING IN AMERICANS

In December, I wrote a post noting that NSA personnel performing analysis on PATRIOT-authorized metadata (both phone or Internet) can choose to contact chain on just that US-collected data, or — in what's call a "federated query" — on foreign collected data, collected under Executive Order 12333, as well. It also appears (though I'm less certain of this) that analysts can do contact chains that mix phone and Internet data, which presumably is made easier by the rise of smart phones.

Section 215 is just a small part of the dragnet

This is one reason I keep complaining that journalists reporting the claim that NSA only collects 20-30% of US phone data need to specify they're talking about just Section 215 collection. Because we know, in part because Richard Clarke said this explicitly at a Senate Judiciary Committee hearing last month, that Section "215 produces a small percentage of the overall data that's collected." At the very least, the EO 12333 data will include the domestic end of any foreign-to-domestic calls it collects, whether made via land line or cell. And that doesn't account for any metadata acquired from GCHQ, which might include far more US person data.

The Section 215 phone dragnet is just a small part of a larger largely-integrated global dragnet, and even the records of US person calls and emails in that dragnet may derive from multiple different authorities, in addition to the PATRIOT Act ones.

SPCMA provided NSA a second way to contact chain on US person identifiers

With that background, I want to look at one part of that dragnet: "SPCMA," which stands for "Special Procedures Governing Communications Metadata Analysis," and which (the screen capture above shows) is one way to access the dragnet of US-collected ("1st person") data. SPCMA provides a way for NSA to include US person data in its analysis of foreign-collected intelligence.

According to what is currently in the public record, SPCMA dates to Ken Wainstein and Steven Bradbury's efforts in 2007 to end some limits on NSA's non-PATRIOT authority metadata analysis involving US persons. (They don't call it SPCMA, but the name of their special procedures match the name used in later years; the word, "governing," is for some reason not included in the acronym)

Wainstein and Bradbury were effectively adding a second way to contact chain on US person data.

They were proposing this change 3 years after Collen Kollar-Kotelly permitted the collection and analysis of domestic Internet metadata and 1 year after Malcolm Howard permitted the collection and analysis of domestic phone metadata under PATRIOT authorities, both with some restrictions, By that point, the NSA's FISC-authorized Internet metadata program had already violated — indeed, was still in violation — of Kollar-Kotelly's category restrictions on Internet metadata collection; in fact, the program never came into compliance until it was restarted in 2010.

By treating data as already-collected, SPCMA got around legal problems with Internet metadata

Against that background, Wainstein and Bradbury requested newly confirmed Attorney General Michael Mukasey to approve a change in how NSA treated metadata collected under a range of other authorities (Defense Secretary Bob Gates had already approved the change). They argued the change would serve to make available foreign intelligence information that had been unavailable because of what they described as an "over-identification" of US persons in the data set.

> NSA's present practice is to "stop" when a chain hits a telephone number or address believed to be used by a United States person. NSA believes that it is over-identifying numbers and addresses that belong to United States persons and that modifying its practice to chain through all telephone numbers and addresses, including those reasonably believed to be used by a United States person, will yield valuable foreign intelligence information primarily concerning non-United States persons outside the United States. It is not clear, however, whether NSA's current procedures permit chaining through a United States telephone number, IP address or e-mail address.

They also argued making the change would pave the way for sharing more metadata analysis with CIA and other parts of DOD.

The proposal appears to have aimed to do two things. First, to permit the same kind of contact chaining — including US person data — authorized under the phone and Internet dragnets, but using data collected under other authorities (in 2007, Wainstein and Bradbury said some of the data would be collected under traditional FISA). But also to do so without the dissemination restrictions imposed by FISC on those PATRIOT-authorized dragnets.

In addition (whether this was one of the goals

or not), SPCMA defined metadata in a way that almost certainly permitted contact chaining on metadata not permitted under Kollar-Kotelly's order.

> "Metadata" also means (1) information about the Internet-protocol (IP) address of the computer from which an e-mail or other electronic communication was sent and, depending on the circumstances, the IP address of routers and servers on the Internet that have handled the communication during transmission; (2) the exchange of an IP address and e-mail address that occurs when a user logs into a web-based e-mail service; and (3) for certain logins to web-based e-mail accounts, inbox metadata that is transmitted to the user upon accessing the account.

Some of this information — such as the web-based email exchange — almost certainly would have been excluded from Kollar-Kotelly's permitted categories because it would constitute content, not metadata, to the telecoms collecting it under PATRIOT Authorities.

Wainstein and Bradbury appear to have gotten around that legal problem — which was almost certainly the legal problem behind the 2004 hospital confrontation — by just assuming the data was already collected, giving it a sort of legal virgin birth.

Doing so allowed them to distinguish this data from Pen Register data (ironically, precisely the authority Kollar-Kotelly relied on to authorize PATRIOT-authorized Internet metadata collection) because it was no longer in motion.

> First, for the purpose of these provisions, "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing or signaling information." 18 U.S.C. § 3127(3); 50 U.S.C. § 1841 (2). When NSA

> will conduct the analysis it proposes, however, the dialing and other information will have been already recorded and decoded. Second, a "trap and trace device" is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing and signaling information." 18 U.S.C. § 3127(4); 50 U.S.C. § 1841(2). Again, those impulses will already have been captured at the point that NSA conducts chaining. Thus, NSA's communications metadata analysis falls outside the coverage of these provisions.

And it allowed them to distinguish it from "electronic surveillance."

> The fourth definition of electronic surveillance involves "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication …. " 50 U.S.C. § 1802(f)(2). "Wire communication" is, in turn, defined as "any communication while it is being carried by a wire, cable, or other like com1ection furnished or operated by any person engaged as a common carrier …. " !d. § 1801 (1). The data that the NSA wishes to analyze already resides in its databases. The proposed analysis thus does not involve the acquisition of a communication "while it is being carried" by a connection furnished or operated by a common carrier.

This legal argument, it seems, provided them a way to carve out metadata analysis under DOD's secret rules on electronic surveillance, distinguishing the treatment of this data from "interception" and "selection."

> For purposes of Procedure 5 of DoD

> Regulation 5240.1-R and the Classified Annex thereto, contact chaining and other metadata analysis don't qualify as the "interception" or "selection" of communications, nor do they qualify as "us[ing] a selection term," including using a selection term "intended to intercept a communication on the basis of … [some] aspect of the content of the communication."

This approach reversed an earlier interpretation made by then Counsel of DOJ's Office of Intelligence and Policy Review James A Baker.

Baker may play an interesting role in the timing of SPCMA. He had just left in 2007 when Bradbury and Wainstein proposed the change. After a stint in academics, Baker served as Verizon's Assistant General Counsel for National Security (!) until 2009, when he returned to DOJ as an Associate Deputy Attorney General. Baker, incidentally, got named FBI General Counsel last month.

NSA implemented SPCMA as a pilot in 2009 and more broadly in 2011

It wasn't until 2009, amid NSA's long investigation into NSA's phone and Internet dragnet violations that NSA first started rolling out this new contact chaining approach. I've noted that the rollout of this new contact-chaining approach occurred in that time frame.

Comparing the name …

> SIGINT Management Directive 424 ("SIGINT Development-Communications Metadata Analysis") provides guidance on the NSA/CSS implementation of the "Department of Defense **Supplemental Procedures Governing Communications Metadata Analysis" (SPCMA)**, as approved by the U.S. Attorney General and the Secretary of Defense. [my emphasis]

And the description of the change …

> Specifically, these new procedures **permit contact chaining, and other analysis, from and through any selector, irrespective of nationality or location, in order to follow or discover valid foreign intelligence targets**. (Formerly analysts were required to determine whether or not selectors were associated with US communicants.) [emphasis origina]

,,, Make it clear it is the same program.

NSA appears to have made a few changes in the interim. In 2007, Wainstein and Bradbury said it might include FISA-collected data and "other authorities" (suggesting they might use STELLAR WIND data). In its 2011 rollout, it reportedly applied only to EO 12333 collected data.

In addition, the original proposal focused primarily on contact-chaining. In the implementation, SPCMA permitted "other analysis" as well.

The later (internal to NSA) description also makes it much more clear the point is to identify ties between foreign targets and Americans.

> In the first place it allows NSA to discover and track connections between foreign intelligence targets and possible 2nd Party or US communicants.

Finally, as implemented, SPCMA required analysts to adhere to existing dissemination rules; given that this is EO 12333 data, that still would permit broader dissemination than under the PATRIOT-authorized dragnet, but may not have resulted in as unfettered sharing with the CIA as NSA had wanted.

Additionally, in what would have been true from the start but was made clear in the roll-out, NSA could use this contact chaining for any

foreign intelligence purpose. Unlike the PATRIOT-authorized dragnets, it wasn't limited to al Qaeda and Iranian targets. NSA required only a valid foreign intelligence justification for using this data for analysis.

> **The primary new responsibility is the requirement:**

- **to enter a foreign intelligence (FI) justification for making a query or starting a chain,** [emphasis original]

Now, I don't know whether or not NSA rolled out this program because of problems with the phone and Internet dragnets. But one source of the phone dragnet problems, at least, is that NSA integrated the PATRIOT-collected data with the EO 12333 collected data and **applied the protections for the latter authorities** to both (particularly with regards to dissemination). NSA basically just dumped the PATRIOT-authorized data in with EO 12333 data and treated it as such. Rolling out SPCMA would allow NSA to use US person data in a dragnet that met the less-restrictive minimization procedures.

But, as I said, at least until late 2011, from when the screen caption above was taken, SPCMA metadata analysis was available from the very same interface as PATRIOT-authority analysis (as well as "normal," which may be EO 12333 data excluding US person identifiers). As I've noted in the past, that same training program coached analysts how to re-run PATRIOT-authority queries to obtain EO 12333 results that could be more broadly shared.

That "other analysis" permitted under SPCMA

I'm really just beginning to understand SPCMA and how it works. I certainly have no idea how broadly NSA collects the EO 12333 data that gets dumped into it, and to what degree it replicates

domestically collected data. At best, it could only include data that companies like Verizon made available off shore, but it would also include a lot of data not collected under the PATRIOT authorities.

But, especially given discussions lately about difficulties NSA has integrating cell data because of geolocation information, I'm particularly interested that one of NSA's pilot co-traveler programs, CHALKFUN, works with SPCMA.

> Chalkfun's Co-Travel analytic computes the date, time, and network location of a mobile phone over a given time period, and then looks for other mobile phones that were seen in the same network locations around a one hour time window. When a selector was seen at the same location (e.g., VLR) during the time window, the algorithm will reduce processing time by choosing a few events to match over the time period. **Chalkfun is SPCMA enabled1.**

> 1 (S//SI//REL) SPCMA enables the analytic to chain "from," "through," or "to" communications metadata fields without regard to the nationality **or location** of the communicants, and users may view those same communications metadata fields in an unmasked form. [my emphasis]

Now, aside from what this says about the dragnet database generally (because this makes it clear there is location data in the EO 12333 data available under SPCMA, though that was already clear), it makes it clear there is a way to geolocate US persons — because the entire point of SPCMA is to be able to analyze data including US persons, without even any limits on their location (meaning they could be in the US).

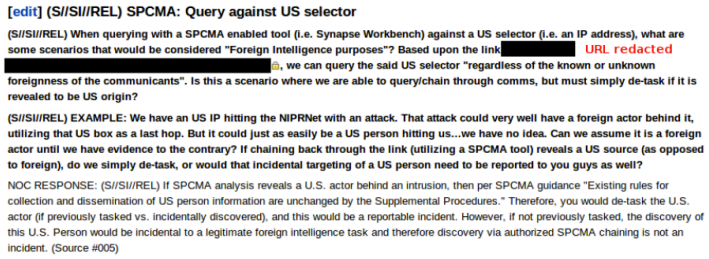
I think it marginally possible NSA might be

forced to deactivate such functions if it is forced to do so domestically more generally. But at least in October 2012 (so long after *US v. Jones*), it appears NSA permitted geolocation of US persons within the US using CHALKFUN under SPCMA.

Again, I'm just beginning to understand how SPCMA has been enacted. But it seems to provide a nice big loophole to analyze US person metadata under guidelines that are far more permissive than the PATRIOT-authorized authorities. Including, at least until 2012, geolocation. There's a lot of data that won't be available under this program (and NSA has to claim it is aiming to collect non-US data under EO 12333).

But what data it does get collected … "incidentally" … gets exposed to far more analysis than that under the PATRIOT authorized dragnets.

Update: This passage, from documents released in Glenn Greenwald's latest, shows how SPCMA still requires queries to target a foreign entity (though you can see how they coach using a foreign tasker so as to permit the chaining).



[edit] (S//SI//REL) SPCMA: Query against US selector

(S//SI//REL) When querying with a SPCMA enabled tool (i.e. Synapse Workbench) against a US selector (i.e. an IP address), what are some scenarios that would be considered "Foreign Intelligence purposes"? Based upon the link [redacted] URL redacted [redacted], we can query the said US selector "regardless of the known or unknown foreignness of the communicants". Is this a scenario where we are able to query/chain through comms, but must simply de-task if it is revealed to be US origin?

(S//SI//REL) EXAMPLE: We have an US IP hitting the NIPRNet with an attack. That attack could very well have a foreign actor behind it, utilizing that US box as a last hop. But it could just as easily be a US person hitting us…we have no idea. Can we assume it is a foreign actor until we have evidence to the contrary? If chaining back through the link (utilizing a SPCMA tool) reveals a US source (as opposed to foreign), do we simply de-task, or would that incidental targeting of a US person need to be reported to you guys as well?

NOC RESPONSE: (S//SI//REL) If SPCMA analysis reveals a U.S. actor behind an intrusion, then per SPCMA guidance "Existing rules for collection and dissemination of US person information are unchanged by the Supplemental Procedures." Therefore, you would de-task the U.S. actor (if previously tasked vs. incidentally discovered), and this would be a reportable incident. However, if not previously tasked, the discovery of this U.S. Person would be incidental to a legitimate foreign intelligence task and therefore discovery via authorized SPCMA chaining is not an incident. (Source #005)