2008'S NEW AND IMPROVED EO 12333: SHARING SIGINT

As part of my ongoing focus on Executive Order 12333, I've been reviewing how the Bush Administration changed the EO when, shortly after the passage of the FISA Amendments Act, on July 30, 2008, they rolled out a new version of the order, with little consultation with Congress. Here's the original version Ronald Reagan issued in 1981, here's the EO making the changes, here's how the new and improved version from 2008 reads with the changes.

While the most significant changes in the EO were — and were billed to be — the elaboration of the increased role for the Director of National Intelligence (who was then revolving door Booz executive Mike McConnell), there are actually several changes that affected NSA.

Perhaps the most striking of those is that, even while the White House claimed "there were very, very few changes to Part 2 of the order" — the part that provides protections for US persons and imposes prohibitions on activities like assassinations — the EO actually replaced what had been a prohibition on the dissemination of SIGINT pertaining to US persons with permission to disseminate it with Attorney General approval.

The last paragraph of 2.3 — which describes what data on US persons may be collected — reads in the original,

> In addition, agencies within the Intelligence Community may disseminate information, **other than information derived from signals intelligence**, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can

> be retained by it.

The 2008 version requires AG and DNI approval for such dissemination, but it affirmatively permits it.

> In addition, elements of the Intelligence Community may disseminate information to each appropriate element within the Intelligence Community for purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it, **except that information derived from signals intelligence may only be disseminated or made available to Intelligence Community elements in accordance with procedures established by the Director in coordination with the Secretary of Defense and approved by the Attorney General**.

Given that the DNI and AG certified the minimization procedures used with FAA, their approval for any dissemination under that program would be built in here; they have already approved it! The same is true of the SPCMA — the EO 12333 US person metadata analysis that had been approved by both Attorney General Mukasey and Defense Secretary Robert Gates earlier that year. Also included in FISA-specific dissemination, the FBI had either just been granted, or would be in the following months, permission — in minimization procedures approved by both the DNI and AG — to conduct back door searches on incidentally collected US person data.

In other words, at precisely the time when at least 3 different programs expanded the DNI and AG approved SIGINT collection and analysis of US person data, EO 12333 newly permitted the dissemination of that information.

And a more subtle change goes even

further. Section 2.5 of the EO delegates authority to the AG to "approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes." In both the original and the revised EO, that delegation must be done within the scope of FISA (or FISA as amended, in the revision). But in 1981, FISA surveillance had to be "conducted in accordance with that Act [FISA], **as well as this Order**," meaning that the limits on US person collection and dissemination from the EO applied, on top of any limits imposed by FISA. The 2008 EO dropped the last clause, meaning that such surveillance **only** has to comply with FISA, and not with other limits in the EO.

That's significant because there are at least three things built into known FISA minimization procedures — the retention of US person data to protect property as well as life and body, the indefinite retention of encrypted communications, and the broader retention of "technical data base information" — that does not appear to be permitted under the EO's more general guidelines but, with this provision, **would** be permitted (and, absent Edward Snowden, would also be hidden from public view in minimization procedures no one would ever get to see).

Given that Section 2.5 would thus permit the collection of US person data so long as it was dubbed "technical data base information," consider the way the intelligence mandate for a number of elements of the intelligence community (including DIA, FBI, DOD and its subcomponents generally, Coast Guard, NRO, NGA, and INR, in addition to NSA, but curiously not the CIA) were newly laid out. Each of these elements is permitted to collect intelligence to support national **and departmental** missions. Here's how that language appears as it applies to the NSA:

> Collect (including through clandestine

> means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions;
>
> [snip]
>
> Provide signals intelligence support for national and departmental requirements and for the conduct of military operations;

Curiously, this change comes with the elimination of the 1981 clause authorizing NSA's "Conduct of research and development to meet the needs of the United States for signals intelligence and communications security" (though there is a similar clause in the 2008 EO applying to both the Intelligence Community as a whole and DOD specifically, which would both apply to NSA). NSA still collects and uses the data it needs to conduct research to advance the SIGINT mission, it appears, but as it seems in the 2008 EO, it does so in the name of advancing the Department's goals, not the nation's.

In 1981, only DOD had such a departmental mandate. Extending it to these other agencies and departments seems to give them a recursive purpose, the mandate to collect intelligence to serve their own department.

And all this comes in an EO that seems to envision SIGINT playing a bigger role in US intelligence (which makes sense, given that's what we know to have happened). The 1981 EO explicitly calls for a balance between, "technical collection efforts and other means." The 2008 EO eliminates that.

In addition, the 2008 description of both the CIA and FBI's roles limits their focus to human and human-enabled sources (which is particularly curious given that FBI actually has a key role in SIGINT collection).

> (A) The Director of the Federal Bureau of Investigation shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities inside the United States;
>
> (B) The Director of the Central Intelligence Agency shall coordinate the clandestine collection of foreign intelligence collected through human sources or through human-enabled means and counterintelligence activities outside the United States;

At the same time, the revised EO designates the Director of NSA as the functional manager for SIGINT, seemingly both within and outside of the US.

As I said, none of that should be surprising: it reflects both what we knew before last June, and has been reinforced with much of what we've learned with the Snowden leaks. But it does reflect a codification of that change that I don't think got much notice at the time, even in spite of the EO's revision coming so quickly on the heels of FAA.

There are two more items of interest that affect the potential scope of information sharing, and this applies to both NSA and other elements of the intelligence community (including, to the extent permitted by law, CIA).

First, in one of the changes the Bush Administration hailed at the time, the EO envisions information sharing outside of the Federal government, to state, local, and tribal governments, and to the private sector.

> (f) State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests. Our national intelligence effort should take

> into account the responsibilities and requirements of State, local, and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.

This language is repeated several times in the EO.

In a far more subtle change, section 2.6(d) allows intelligence entities to cooperate not just with domestic law enforcement, but also with "other civil authorities" so long as it is not otherwise legally precluded. I can only begin to grasp what the Bush Administration had in mind with this. But at least in the case of NSA, in the face of endless cyber-fearmongering, I can imagine it might support NSA partnering with civil agencies overseeing critical infrastructure (to the extent that that infrastructure is owned by civil authorities and not the private sector).

In 2008, even as the Bush Administration insisted that protections on US person data didn't change with EO 12333's revision, it appears they did change those protections to allow the dissemination of SIGINT on US persons, potentially even to local governments and private entities.

I suspect many, perhaps most, of the changes affecting NSA were not actually new changes. As we know, John Yoo had pixie dusted EO 12333 to hide what the Bush Administration was doing with SIGINT. And at least as late as December 2007, Sheldon Whitehouse believed that pixie dust to remain in effect. So I think it likely that the NSA-related changes simply reflect what Bush had been doing since 2001 in any case.

But in retrospect, the changes to EO 12333 might have raised more alarm about the growing role of the NSA and the dissemination of the data on US persons it collected.

NSA MAY NOT VOYEURISTICALLY PORE THROUGH EMAIL BUT GCHQ VOYEURISTICALLY PORES THROUGH WEBCAM PICTURES

Back in James Clapper's very first attempt to dismiss his lies to Ron Wyden, he said,

> "What I said was, the NSA does not voyeuristically pore through U.S. citizens' e-mails. I stand by that," Clapper told National Journal in a telephone interview.

Apparently, however, NSA's partner goes one step beyond that, with NSA"s assistance: GCHQ pores through bulk collected webcam photos, including those of US persons, of Yahoo's users.

> Britain's surveillance agency GCHQ, with aid from the National Security Agency, intercepted and stored the webcam images of millions of internet users not suspected of wrongdoing, secret documents reveal.
>
> GCHQ files dating between 2008 and 2010 explicitly state that a surveillance program codenamed Optic Nerve collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not.

This includes the 3 to 11% of images that show nudity.

> Sexually explicit webcam material proved to be a particular problem for GCHQ, as one document delicately put it: "Unfortunately … it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography."
>
> The document estimates that between 3% and 11% of the Yahoo webcam imagery harvested by GCHQ contains "undesirable nudity".

Given past discussions of circumcision in regards to terrorist suspects, it's only a matter of time before GCHQ defends its nudity stash because such evidence can be proof of radicalization (heh). Plus, we already know that NSA and GCHQ like to use targets' online porn habits to discredit them.

Coming soon to an "oversight" hearing near you: James Clapper refuses to talk about this invasion of an American company's customers' privacy because it occurs under EO 12333 and liaison partnerships, and therefore is not subject to Congressional oversight.

JACK GOLDSMITH'S STILL ACTIVE PRESIDENTIAL DRAGNET

AUTHORIZATION

In the follow-up questions for CIA General Counsel nominee Caroline Krass, Ron Wyden asked a series of his signature loaded questions. With it, he pointed to the existence of still-active OLC advice — Jack Goldsmith's May 6, 2004 memo on Bush's illegal wiretap program — supporting the conduct of a phone (but not Internet) dragnet based solely on Presidential authorization.

He started by asking "Did any of the redacted portions of the May 2004 OLC opinion address bulk telephony metadata collection?

Krass largely dodged the question — but did say that "it would be appropriate for the May 6, 2004 OLC opinion to be reviewed to determine whether additional portions of the opinion can be declassified."

In other words, the answer is (it always is when Wyden asks these questions) "yes."

This is obvious in any case, because Goldsmith discusses shutting down the Internet dragnet program, and spends lots of time discussing locating suspects.

Wyden then asked if the opinion relied on something besides FISA to conduct the dragnet.

> [D]id the OLC rely at that time on a statutory basis other than the Foreign Intelligence Surveillance Act for the authority to conduct bulk telephony metadata collection?

Krass dodged by noting the declassification had not happened so she couldn't answer.

But the 2009 Draft NSA IG Report makes it clear the answer is yes: NSA collected such data, both before and after the 2004 hospital showdown, based solely on Presidential authorization (though on occasion DOJ would send letters to the telecoms to reassure them both the metadata

and content collection was legal).

Finally, Wyden asks the kicker: “Has the OLC taken any action to withdraw this opinion?”

Krass makes it clear the memo is still active, but assures us it’s not being used.

> OLC generally does not reconsider the status of its prior opinions in the absence of a practical need by an element of the Executive Branch to know whether it can rely upon the advice in connection with its ongoing operations. My understanding is that any continuing NSA collection activities addressed in the May 6, 2004 opinion are being conducted pursuant to authorization by the Foreign Intelligence Surveillance Court, and thus do not rely on the advice of the opinion.

Of course, just yesterday both Dianne Feinstein and Mark Udall made it clear that no one at DOJ is paying close attention to EO 12333 — that is, Presidentially — authorized activities. So how would she know?

One way or another, the Executive Branch still has OLC sanction to conduct a phone dragnet off the books, using only Presidential authorization.

The question is whether, in addition to pointing to this authorization, Wyden is also suggesting that the Executive is currently using it.

(h/t to KH for alerting me that the QFRs had been posted)

DOES ACTING NATIONAL

SECURITY DIVISION HEAD JOHN CARLIN KNOW ABOUT FISA SECTIONS 703 AND 704?

There were several curious exchanges in today's hearing for Acting National Security Division AAG John Carlin to become the official AAG.

I'll start with this exchange. (After 1:01, my transcription)

> Udall: I want to talk about Executive Order 12333, with which you're familiar. I understand that the collection, retention, or dissemination of information about US persons is prohibited under Executive Order 12333 except under certain procedures approved by the Attorney General. But this doesn't mean that US person information isn't mistakenly collected or obtained and then disseminated outside these procedures, so take this example. Let's say the NSA's conducting what it believes to be foreign to foreign collection under EO 12333 but discovers in the course of this collection that it also incidentally collected a vast trove of US person information. That US person collection should now have FISA protections. What role does the NSD have in overseeing any collection, retention, or dissemination of US person information that might occur under that executive order?
>
> Carlin: Senator, so, generally the intelligence activities that NSA would conduct under its authorities pursuant to EO 12333 would be done pursuant to a series of guidelines that were approved by the Attorney General and then ultimately implemented through

> additional policies and procedures by NSA. But the collection activities that occur pursuant to 12333, if there was incidental collection, would be handled through a different set of oversight mechanisms than the Departments—by the Office of Compliance, the Inspector General there, the General Counsel there, and the Inspector General and General Counsel's office for the Intelligence Community writ large, as well as reporting to these committees as appropriate.
>
> Udall: So you don't see a role for NSD in ensuring that that data is protected under FISA?
>
> Carlin: Under FISA, no, under FISA we would have a direct role, so if it was under, if it was collection that was pursuant to the FISA statutes, so collection targeted at US persons, for example, or collection targeted at certain non-US persons overseas that was collected domestically such as pursuant to the 702 collection program. That would fall within the scope of the National Security Division. That's information that – and oversight that we conduct through our oversight section in conjunction with the agencies. We would have the responsibility in terms of informing, of working with them to inform the court if there were any compliance incidents and making sure those compliance incidents were addressed.
>
> Udall: My time's obviously expired, but I think you don't understand where I'm coming from here. One is to make sure the DOJ and you in your capacity have the most accurate information so you can represent United States of America and our citizens in the best possible way, and secondly that you have an additional

> role to play in providing additional oversight. Those are all tied to having information that's factual, that's based on what happened, and I'm going to continue to look for ways possible to make sure that's what does happen, whether it's under the auspices of the IC or the DOJ. You all have a responsibility to protect the Bill of Rights.

Udall asks Carlin about a "vast trove" of US person data collected under the guise of EO 12333, and asks whether NSD would have a role in protecting it under FISA.

Carlin responds by saying NSD wouldn't have any role; only NSA and ODNI have oversight over EO 12333 compliance with the Attorney General approved guidelines.

At first, I thought Udall didn't get Carlin's point — that this data would get no FISA protection. (Earlier in the hearing, Dianne Feinstein had even pointed out EO 12333 collection gets less oversight, and suggested maybe NSD should play a role in EO 12333 compliance.)

But upon review, Udall may have been suggesting something else (I have a question in with his office seeking clarity on this point).

By all appearances, this was **content**, not metadata (under SPCMA, metadata collection is considered fair game).

US person content cannot be collected overseas — not intentionally at least — outside the purview of FISA sections 703 and 704.

And while admittedly I have yet to meet a lawyer who has been able to explain precisely how those statutes work, and while the White House has given particularly crazy answers on this point, it seemed that Carlin couldn't even conceive of a way that US person content collected overseas would be protected under FISA.

He may simply be reflecting NSA policy that if they collect US person content overseas under EO 12333, they call it incidental and therefore never have to consider the FISA implications. And that may well be what the letter of the law provides (in which case I'm sure NSA never ever exploits that loophole, nosirree bob).

But he seemed completely unfamiliar with the concept that, under FISA Amendments Act, US persons do get FISA protection overseas.

Really?

Update: According to Udall's spokesperson, he wasn't specifically thinking of 703 and 704, but asking whether this data "should" fall under FISA and therefore under NSD's oversight.

BETWEEN TWO ENDS OF THE WIKILEAKS INVESTIGATION: PARALLEL CONSTRUCTING THE FBI'S SECRET AUTHORITIES

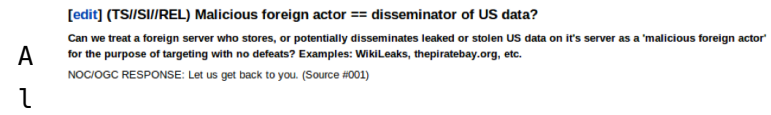
Two pieces of news on the government's investigation of WikIleaks came out yesterday.

At the Intercept, Glenn Greenwald reported:

- In 2010, a "Manhunting Timeline" described efforts to get another country to prosecute what it called the

"rogue" website

- In a targeting scenario dating to July 25, 2011, the US' Targeting and General Counsel personnel responded to a question about targeting WikiLeaks' or Pirate Bay's server by saying they'd have to get back to the questioner
- In 2012, GCHQ monitored WikiLeaks – including its US readers – to demonstrate the power of its ANTICRISIS GIRL initiative


[edit] (TS//SI//REL) Malicious foreign actor == disseminator of US data?

Can we treat a foreign server who stores, or potentially disseminates leaked or stolen US data on it's server as a 'malicious foreign actor' for the purpose of targeting with no defeats? Examples: WikiLeaks, thepiratebay.org, etc.

NOC/OGC RESPONSE: Let us get back to you. (Source #001)

Also yesterday, Alexa O'Brien reported (and contextualized with links back to her earlier extensive reporting):

- The grand jury investigation of WikiLeaks started at least as early as September 23, 2010
- On January 4, 2011 (21 days after the December 14, 201 administrative subpoena for Twitter records on Appelbaum and others), DOJ requested Jacob Appelbaum's Gmail records
- On April 15, 2011, DOJ requested Jacob Appelbaum's Sonic records

Now, as O'Brien lays out in her post, at various times during the investigation of WikiLeaks, it

has been called a Computer Fraud and Abuse investigation, an Espionage investigation, and a terrorism investigation.

Which raises the question why, long after DOJ had deemed the WikiLeaks case a national security case that under either the terrorism or Espionage designation would grant them authority to use tools like National Security Letters, they were still using subpoenas that were getting challenged and noticed to Appelbaum? Why, if they were conducting an investigation that afforded them all the gagged orders they might want, were they issuing subpoenas that ultimately got challenged and exposed?

Before you answer "parallel construction," lets reconsider something I've been mulling since the very first Edward Snowden disclosure: the secret authority DOJ and FBI (and potentially other agencies) used to investigate not just WikiLeaks, but also WikiLeaks' supporters.

Back in June 2011, EPIC FOIAed DOJ and FBI (but not NSA) for records relating to the government's investigation of WikiLeaks supporters.

> EPIC's FOIA asked for information designed to expose whether innocent readers and supporters of WikiLeaks had been swept up in the investigation. It asked for:
>
> > 1. *All records regarding any individuals* ***targeted for surveillance for support for or interest in*** *WikiLeaks;*
> > 2. *All records regarding* ***lists of names of***

individuals *who have demonstrated support for or interest in WikiLeaks;*

3. *All records of any* ***agency communications*** *with Internet and social media companies including, but not limited to Facebook and Google, regarding* ***lists of individuals*** *who have demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and*
4. *All records of any* ***agency communications*** *with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding* ***lists of individuals*** *who have*

> > *demonstrated, through monetary donations or other means, support or interest in WikiLeaks. [my emphasis]*

In their motion for summary judgment last February, DOJ said a lot of interesting things about the records-but-not-lists they might or might not have and generally subsumed the entire request under an ongoing investigation FOIA exemption.

Most interesting, however, is in also claiming that some statute prevented them from turning these records over to EPIC, they refused to identify the statute they might have been using to investigate WikiLeaks' supporters.

> All three units at DOJ — as reflected in declarations from FBI's David Hardy, National Security Division's Mark Bradley, and Criminal Division's John Cunningham — claimed the files at issue were protected by statute.
>
> None named the statute in question. All three included some version of this statement, explaining they could only name the statute in their classified declarations.
>
> > The FBI has determined that an Exemption 3 statute applies and protects responsive information from the pending investigative files from disclosure. However, to disclose which statute or further discuss its application publicly would undermine interests protected by Exemption

> > 7(A), as well as by the withholding statute. I have further discussed this exemption in my in camera, ex parte declaration, which is being submitted to the Court simultaneously with this declaration
>
> In fact, it appears the only reason that Cunningham submitted a sealed declaration was to explain his Exemption 3 invocation.
>
> And then, as if DOJ didn't trust the Court to keep sealed declarations secret, it added this plaintive request in the motion itself.
>
> > Defendants respectfully request that the Court not identify the Exemption 3 statute(s) at issue, or reveal any of the other information provided in Defendants' ex parte and in camera submissions.
>
> DOJ refuses to reveal precisely what EPIC seems to be seeking: what kind of secret laws it is using to investigate innocent supporters of WikiLeaks.

Invoking a statutory exemption but **refusing** to identify the statute was, as far as I've been able to learn, unprecedented in FOIA litigation.

The case is still languishing at the DC District.

I suggested at the time that the statute in question was likely Section 215; I suspected at the time they refused to identify Section 215 because they didn't want to reveal what Edward Snowden revealed for them four months later: that the government uses Section 215 for bulk collection.

While they may well have used Section 215 (particularly to collect records, if they did collect them, from Visa, MasterCard, and PayPal — but note FBI, not NSA, would have wielded the Section 215 orders in that case), they couldn't have used the NSA phone dragnet to identify supporters unless they got the FISC to approve WikiLeaks as an associate of al Qaeda (update: Or got someone at NSA's OGC to claim there were reasons to believe WikiLeaks was associated with al Qaeda). They could, however, have used Section 215 to create their own little mini WikiLeaks dragnet.

For the same reason, they could not have used the PR/TT-authorized Internet dragnet to identify those who might have communicated with Assange or Bradley Manning Support Group members (though by this point they already had David House's computer with a membership list of the latter on it). The domestic Internet dragnet was operational, after having been shut down already, between at least October 2010 until the end of 2011. But it, like the Section 215 dragnet, was apparently limited to terrorist identifiers.

Finally, we know under Special Procedures (SPCMA) approved in 2008 and piloted in 2009, NSA claimed the authority to track which Americans were in contact with foreign targets like Julian Assange, using communications data collected somewhere offshore. Significantly, there is no restriction to terrorism uses for SPCMA; analysts need only cite a foreign intelligence purpose. In an Espionage investigation of WikiLeaks after the adoption of SPCMA, all US person metadata collected internationally off the WikiLeaks server would have been fair game (though NSA would have to comply with dissemination limitations).

There is no authority permitting this SPCMA collection. NSA and DOD and DOJ simply claimed it under Article II. If that's what they're using to investigate WikiLeaks' supporters, I can imagine why DOJ wouldn't want to reveal that

in a public filing in a FOIA case!

Particularly given the way at least two providers challenged either the gags or these criminal subpoenas themselves, there is zero reason to believe DOJ was doing anything other than providing some other claimed source for the evidence they wanted to submit to the grand jury (though there are some interesting NSLs that got challenged by various service providers in that same 2011 time frame, including the presumed Credo one).

So there are 3 details about the US investigation into WikiLeaks during 2011 of interest:

- By June 2011, they were using an authority to conduct such an investigation that they refuse to disclose
- They were, through that very same period, issuing criminal subpoenas that providers were challenging
- NSA refused to say, in writing and after that EPIC FOIA was filed, whether analysts could incidentally collect US person communications to the WikiLeaks server based on a claim it was a malicious actor

Given all that the government has declassified — including references to SPCMA — I wonder if DOJ would now be willing to tell EPIC what statute — or lack thereof — it is hiding behind.

Updated: Changed reference to O'Brien's reporting because it said the opposite of what I

intended to say.

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

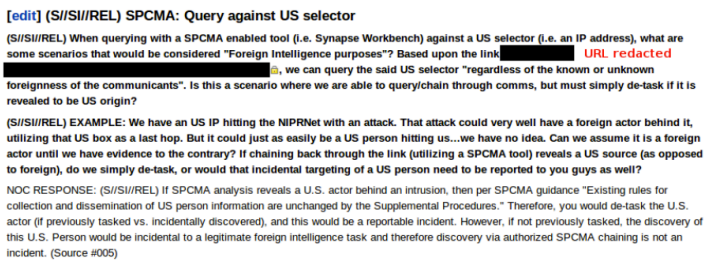
geolocate US persons — because the entire point of SPCMA is to be able to analyze data including US persons, without even any limits on their location (meaning they could be in the US).

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)

WHY TICE?

It has taken me a day or so to report that Russell Tice has been subpoenaed, mostly because I'm still puzzling through it. I'm wondering why Tice. Why not other people almost certainly involved with the leaks to Risen and Lichtblau. I mean, I'd bet my hat that James Comey was a source for Eric Lichtblau, but I haven't heard about Comey getting subpoenaed. Why not the former technology manager who seems to be a key source for both Risen and Lichtblau and Harris and Naftali?

> A former technology manager at a major telecommunications company said that since the Sept. 11 attacks, the leading companies in the industry have been storing information on calling patterns and giving it to the federal government to aid in tracking possible terrorists.
>
> "All that data is mined with the cooperation of the government and shared with them, and since 9/11, there's been much more active involvement in that area," said the former manager, a telecommunications expert who did not want his name or that of his former company used because of concern about revealing trade secrets.

He or she must have had clearance and must be senior enough to track down fairly easily. Another real doozy of a witnesses would be Mark Klein, who gave explicit details on the AT&T program to Wired News, which then published those details.

Of course, that's the thing. We don't know whether Tice is the only supposed Risen-Lichtblau source getting subpoenaed, or whether he's simply the only one going public about the fact.

Sibel Edmonds' National Security Whistleblowers Coalition suggests the Tice subpoena relates

specifically to the cases against AT&T currently working their way—or not—through the courts.

> In addition, the timing of the subpoena appears to be more than a little suspect. On July 25, 2006, Judge Matthew Kennelly upheld the government's assertion of the state secrets privilege in *Terkel v. AT&T*. The crucial issue in the case was whether or not the government's program of surveillance had been publicly acknowledged, and Kennelly wrote "the focus should be on information that bears persuasive indication of reliability." If there were reliable public reports of the program then the fact of the program's existence could not be a state secret. Kennelly found that there were no reliable sources of public information about the contested program's existence sufficient to thwart the government's need for secrecy. In other words, the existence of the program had not been conclusively established, and the government therefore had a right to prevent probing into the matter. This stops a case that represented a serious threat to the Bush administration.
>
> Professor William Weaver, NSWBC Senior Advisor, stated: "Russ Tice is the only publicly identified NSA employee connected to the *New York Times* in its December 2005 story publicizing warrantless Bush-ordered surveillance. Tice is also publicly perceived as someone who could authoritatively establish the existence of the program at issue in *Terkel*; Tice could remedy the defect in the plaintiff's case cited by Kennelly that allowed the government's assertion of the state secrets privilege to be successful. Later, on the same day Kennelly's opinion was filed, the Department of Justice sent out Tice's subpoena. The

> date on the subpoena is July 20th, before Kennelly's decision was filed, but the issue in the Terkel case was so pregnant that it would be easy for the government to anticipate the ruling and only issue the subpoena to Tice if necessary. It has now become necessary, and the government seems to be moving to put pressure on Tice not to reveal information that would confirm the electronic surveillance program at issue in *Terkel* by threatening him with investigation and possible indictment."

Though I'd suggest an equally relevant court case and date might be the Hepting v. AT&T case; on July 20th, the same day as Tice's subpoena got written, Judge Walker allowed the Hepting (the Electronic Freedom Federation) case to go forward.

But I'm not entirely convinced. Mostly, I'm not convinced because I don't think Tice is the source for the specific details about tapping into the phone switches. For example, in this Reason interview, Tice talks in well-informed but hypothetical terms about a program resembling what we understand to be the AT&T program.

> If you wanted to, you could suck in an awful lot of information. The biggest constraint you're going to have is the computing power you need to do it. You need to have some huge computers to crunch that kind of stuff. **More than likely you're talking about picking it up in a digital format and analyzing it** depending on how the program is written depending on whether it's audio or digital recognition you're talking about, the computing power is phenomenal for that sort of thing. **Especially if you're talking about mass volumes, if you're talking about hundreds of thousands of, say, telephone**

> **communications or something like that, calls of people just like you and me, like we're talking now.**
>
> Then you have things like, and this is where language specialists come in, linguists who specialize in things like accents and inflections and speech patterns and all those things that come into play. Or looking for key phrases or combinations of key words within a block of speech. It becomes, when you add in all the variables, astronomical. [my emphasis]

He then later says he's talking about a program no one knows anything about.

> **REASON: You're referring to what James Risen calls "The Program," the NSA wiretaps that have been reported on?**
>
> **Tice:** No, I'm referring to what I need to tell Congress that no one knows yet, which is only tertiarily connected to what you know about now.

By the time this interview was published, both the Risen and Lichtblau article providing more details on the large-scale collection of data and the Harris and Naftali article had already appeared. They provide pretty specific details of intercepting switches, so it's unlikely that Tice's secret has to do with the AT&T intercept program.

In the same interview, Tice twice says he doesn't think the details of the program he's talking about **should** become public.

> First of all, I don't want this stuff to leak out. I'm not going to tell you or anyone in the press anything that's classified, especially about these programs.
>
> [snip]

> In my case, there's no way the programs I want to talk to Congress about should be public ever, unless maybe in 200 years they want to declassify them. You should never learn about it; no one at the *Times* should ever learn about these things.

Which suggests that Tice's comments on any hypothetical telecom intercept case do not relate to the program he's concerned about, and that his comments are not classified. Tice may be telling reporters there's something big there they still haven't found; he may be providing guidance to understand the programs they've already discovered. Indeed, if you look at how the ABC News story reports he was a source for Risen and Lichtblau,

> But Tice disagrees. He says the number of Americans subject to eavesdropping by the NSA could be in the millions if the full range of secret NSA programs is used.

It appears likely he may have just been one of the people telling Risen and Lichtblau the NSA programs were bigger than they initially reported.

> The National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001, attacks to hunt for evidence of terrorist activity, according to current and former government officials.
>
> The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said. It was collected by tapping

> directly into some of the American telecommunication system's main arteries, they said.

(Though admittedly, if Tice is one of these sources, it suggests he may have given Risen and Lichtblau the general idea of direct intercept from the switches. Though it still seems that that's not the program he's whisteblowing.)

So why Tice, then? FWIW, Tice says he was subpoenaed to cow others into silence.

> This latest action by the government is designed only for one purpose: to ensure that people who witness criminal action being committed by the government are intimidated into remaining silent.

Which might mean this is just harrassment—that Tice hasn't broken any laws, but the government will go after him nevertheless because it will prevent others from coming forward. They'll tar him as a paranoid former employee fired for cause. They'll suggest that anyone questioning the domestic spying programs is just equally crazy.

But I also wonder whether the government isn't trying to scare him from leaking details of the program he says he doesn't want to leak. Or whether it isn't trying to scare other whistleblowers and journalists from reporting on the as-yet unreported programs, the ones that seem to be bubbling just beneath the surface.

The AT&T cases are important because, as class action suits targeting the vacuuming of data, they involve everyone. They defy excuses that, "you only need to worry if you've been doing something you shouldn't be," because the programs target all data going through selected switches. And by targeting publicly traded corporations, they threaten to bring real financial consequences, if not legal ones. (Though TNH's resident realist Kagro X predicts all of them will still get dismissed on State

Secrets grounds, whether at the appellate level or somewhere else.)

But I've got a nagging feeling that we're getting close—close to either the details that prove the known programs have been abused, or to the programs that entail a surveillance so oppressive that even Joe Sixpack will get up in arms over it.