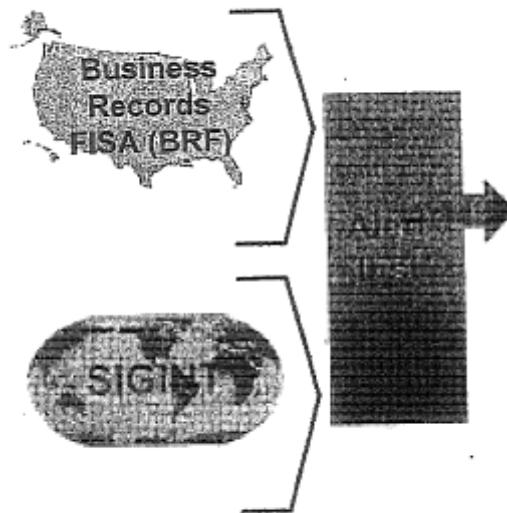


NSA'S DISINGENUOUS CLAIMS ABOUT EO 12333 AND THE FIRST AMENDMENT

Thanks to John Napier Tye's Sunday op-ed, some surveillance watchers are just now discovering EO 12333, which I've written some 50 posts about over the last year.



Back in January, I focused on one of the most alarming disclosures of the 2009 phone dragnet problems, that 3,000 presumed US person identifiers were on an alert list checked against each day's incoming phone dragnet data. That problem – indeed, many of the problems reported at the beginning of 2009 – arose because the NSA dumped their Section 215 phone dragnet data in with all the rest of their metadata, starting at least as early as January 4, 2008. It took at least the better part of 2009 for the government to start tagging data, so the NSA could keep data collected under different authorities straight, though once they did that, NSA trained analysts to use those tags to bypass the more stringent oversight of Section 215.

One thing that episode revealed is that US person data gets collected under EO 12333 (that's how those 3,000 identifiers got on the

alert list), and there's redundancy between Section 215 and E.O. 12333. That makes sense, as the metadata tied to the US side of foreign calls would be collected on collection overseas, but it's a detail that has eluded some of the journalists making claims about the scope of phone dragnet.

Since I wrote that early January post, I've been meaning to return to a remarkable exchange from the early 2009 documents between FISC Judge Reggie Walton and the government. In his order for more briefing, Walton raised questions about tasking under NSA's SIGINT (that is, E.O. 12333) authority.

The preliminary notice from DOJ states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?

The question reveals how little Walton — who had already made the key judgments on the Protect America Act program 2 years earlier — knew about E.O. 12333 authority.

I've put NSA's complete response below the rule (remember "Business Records" in this context is the Section 215 phone dragnet authority). But basically, the NSA responded,

- Even though the alert list included IDs that had not been assessed or did not meet Reasonable Articulate Suspicion of a tie to one of

the approved terrorist groups, they at least had to have foreign intelligence value. And occasionally NSA's counterterrorism people purge the list of non-CT IDs.

- Usually, NSA can only task (a form of targeting!) a US person under a FISA authority.
- Under EO 12333 and other related authorities, NSA can collect SIGINT information for foreign and counterintelligence purposes; its collection, retention, and dissemination of US person is governed by Department of Defense Regulation 5240.1-R and a classified annex. (see page 45 for the unclassified part of this)
- Since 2008, if the NSA wants to target a US person overseas they need to get and comply with a FISA order.
- NSA provides First Amendment protection in two ways – first, by training analysts to spy “with full consideration of the rights of United States persons.”
- NSA provides First Amendment protection under EO 12333 by

prohibiting NSA “from collecting or disseminating information concerning US persons’ ‘domestic activities’ which are defined as ‘activities that take place in the domestic United States that do not involve a significant connection to a foreign power, organization, or person.’”

The First Amendment claims in the last two bullets are pretty weak tea, as they don’t actually address First Amendment issues and contact chaining is, after all, chaining on associations.

That’s all the more true given what we know had already been approved by DOJ. In the last months of 2007, they approved the contact chaining through US person identifiers of already-collected data (including FISA data). They did so by modifying DOD 5240.1 and its classified annex so as to treat what they defined (very broadly) as metadata as something other than interception.

The current DOD procedures and their Classified Annex may be read to restrict NSA’s ability to conduct the desired communications metadata analysis, at least with respect to metadata associated with United States persons. In particular, this analysis may fall within the procedures’ definition of, and thus restrictions on, the “interception” and “selection” of communications. Accordingly, the Supplemental Procedures that would govern NSA’s analysis of communications metadata expressly state that the DOD Procedures and the Classified Annex do

not apply to the analysis of communications metadata. Specifically, the Supplemental Procedures would clarify that “contact chaining and other metadata analysis do not 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.” Once approved, the Supplemental Procedures will clarify that the communications metadata analysis the NSA wishes to conduct is not restricted by the DOD procedures and their Classified Annex.

Michael Mukasey approved that plan just as NSA was dumping all the Section 215 data in with EO 12333 data at the beginning of 2008 (though they did not really roll it out across the NSA until later in 2009).

Nowhere in the government’s self-approval of this alternate contact chaining do they mention First Amendment considerations (or even the domestic activities language included in their filing to Walton). And in the rollout, they explicitly permitted starting chains with identifiers of any nationality (therefore presumably including US person) and approved the use of such contact chaining for purposes other than counterterrorism. More importantly, they expanded the analytical function beyond simple contact chaining, including location chaining.

All with no apparent discussion of the concerns a FISC judge expressed when data from EO 12333 had spoiled Section 215 data.

We will, I expect, finally start discussing how NSA has been using EO 12333 authorities – and how they’ve represented their overlap with FISA authorized collection. This discussion is an important place to start.

(TS//SI//NF) Answer 5: SIGINT Tasking Standard: Although the alert list included telephone identifiers of counterterrorism targets that had not been assessed against the RAS standard [requiring a tie to specific, named terrorist organizations] or had been affirmatively determined by NSA personnel not to meet the RAS standard, such identifiers were not tasked in a vacuum. Whether or not an identifier is assessed against the RAS standard, NSA personnel may not task an identifier for any sort of collection or analytic activity pursuant to NSA's general SIGINT authorities under Executive Order 12333 unless, in their professional analytical judgment, the proposed collection or analytic activity involving the identifier is likely to produce information of foreign intelligence value. In addition, NSA's counterterrorism organization conducted reviews of the alert list two (2) times per year to ensure that the categories (zip codes) used to identify whether telephone identifiers on the alert list remained associated with [redacted] or one of the other target sets covered by the Business Records Order. Also, on occasion the SIGINT Directorate changed an identifier's status from RAS approved to non-RAS approved on the basis of new information available to the Agency.

(U) US Person Tasking: NSA possesses some authority to task telephone identifiers associated with US persons for SIGINT collection. For example, with the US person's consent, NSA may collect foreign communications to, from, or about the US person. In most cases, however, NSA's authority to task a telephone number associated with a US person is regulated by the FISA. For the Court's convenience, a more detailed description of the Agency's SIGINT authorities follows, particularly with respect to the collection and dissemination of information to, from, or about US persons.

(TS//SI//NF) NSA's general SIGINT authorities are provided by Executive Order 12333, as

amended (to include the predecessors to the current Executive Order); National Security Council Intelligence Directive No. 6; Department of Defense Directive 5100.20; and other policy direction. In particular, Section 1.7(c) of Executive Order 12333 specifically authorizes NSA to "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information for foreign intelligence and counterintelligence purposes to support national and departmental missions." However, when executing its SIGINT mission, NSA is only authorized to collect, retain or disseminate information concerning United States persons in accordance with procedures approved by the Attorney General. The current Attorney General approved procedures that NSA follows are contained in Department of Defense Regulation 5240.1-R, and a classified annex to the regulation governing NSA's electronic surveillance activities.

(U) Moreover, some, but not all, of NSA's SIGINT activities are also regulated by the Foreign Intelligence Surveillance Act. For example, since the amendment of the FISA in the summer of 2008, if NSA wishes to direct SIGINT activities against a US person located outside the United States, any SIGINT collection activity against the US person generally would require issuance of an order by the FISC. For SIGINT activities executed pursuant to an order of the FISC, NSA is required to comply with the terms of the order and Court-approved minimization procedures that satisfy the requirements of 50 U.S.C. § 1801(h).

(U) First Amendment Considerations: For the following reasons, targeting a US person solely on the basis of protected First Amendment activities would be inconsistent with restrictions applicable to NSA's SIGINT activities. As part of their annual intelligence oversight training, NSA personnel are required to re-familiarize themselves with these restrictions, particularly the provisions that govern and restrict NSA's handling of

information of or concerning US persons. Irrespective of whether specific SIGINT activities are undertaken under the general SIGINT authority provided to NSA by Executive Order 12333 or whether such activity is also regulated by the FISA, NSA, like other elements of the US Intelligence Community, must conduct its activities "with full consideration of the rights of United States persons." See Section 1.1(a) of Executive Order 12333, as amended. The Executive Order further provides that US intelligence elements must "protect fully the legal rights of all United States persons, including freedoms, civil liberties, and privacy rights guaranteed by Federal law." Id. at Section 1.1(b).

(U) Consistent with the Executive Order's requirement that each intelligence agency develop Attorney General approved procedures that "protect constitutional and other legal rights" (EO 12333 at Section 2.4), DoD Regulation 5240.1-R prohibits DoD intelligence components, including NSA, from collecting or disseminating information concerning US persons' "domestic activities" which are defined as "activities that take place in the domestic United States that do not involve a significant connection to a foreign power, organization, or person." See, e.g., Section C2.2.3 of DoD Regulation 5240.1-R, In light of this language, targeting a US person solely on the basis of protected First Amendment activities would be inappropriate.