34 YEARS LATER, TREASURY IS STILL OPERATING WITHOUT PROCEDURES TO PROTECT AMERICANS UNDER EO 12333

With almost no explanation, PCLOB just released this table ODNI compiled showing the status of procedures Agencies follow to protect US person information when using data obtained under EO 12333. This is something PCLOB has been pushing for since August 2013, when it sent a letter to Attorney General Holder pointing out that some agencies weren't in compliance with the EO.

> As you know, Executive Order 12333 establishes the overall framework for the conduct of intelligence activities by U.S. intelligence agencies. Under section 2.3 of the Executive Order, intelligence agencies can only collect, retain, and disseminate information about U.S. persons if the information fits within one of the enumerated categories under the Order and if it is permitted under that agency's implementing guidelines approved by the Attorney General after consultation with the Director of National Intelligence.
>
> The Privacy and Civil Liberties Oversight Board has learned that key procedures that form the guidelines to protect "information concerning United States person" have not comprehensively been updated, in some cases in almost three decades, despite dramatic changes in information use and technology.

So I assume the release of this table is designed to pressure the agencies that have been

stalling this process.

The immediate takeaway from this table is that, 34 years after Ronald Reagan ordered agencies to have such procedures in Executive Order 12333 and 18 months after PCLOB pushed for agencies to follow the EO, several intelligence agencies still don't have Attorney General approved procedures. Those agencies and the interim procedures they're using are:

The Department of Homeland Security's notoriously shoddy Office of Intelligence and Analysis: Pending issuance of final procedures, I&A is operating pursuant to Interim Intelligence Oversight Procedures, issued jointly by the Under Secretary for Intelligence and Analysis and the Associate General Counsel for Intelligence (April 3, 2008).

United States Coast Guard (USCG)- Intelligence and counterintelligence elements: Pending issuance of final procedures, operating pursuant to Commandant Instruction – COMDINST 3820.12, Coast Guard Intelligence Activities (August 28, 2003).

Department of Treasury Office of Intelligence and Analysis (OIA): Pending issuance of final procedures. While draft guidelines are being reviewed in the interagency approval process, the Office of Intelligence and Analysis conducts intelligence operations pursuant to EO 12333 and statutory responsibilities of the IC element, as advised by supporting legal counsel.

Drug Enforcement Administration, Office of National Security Intelligence (ONSI): Pending issuance of final procedures, operates pursuant to guidance of the Office of Chief Counsel, other guidance, and: Attorney General approved "Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons" (September 23, 2002); Attorney General approved "Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in

the Course of a Criminal Investigation" (September 23, 2002).

I'm not surprised about DHS I&A because — as I noted — most people who track it know that it has never managed to do what it claims it should be doing. And I'm not all that worried about the Coast Guard; how much US person spying are they really doing, after all?

One should always worry about the DEA, and the fact that DEA has only had procedures affecting some of its use of EO 12333 intelligence is par for the course. I mean, limits on what it can share with CIA, but no guidelines on what it can share with FBI? And no guidelines on what it has dragnet collected overseas, where it is very active?

But I'm most troubled by Treasury OIA. In part, that's because it doesn't have anything in place — it has just been operating on EO 12333, apparently, in spite of EO 12333's clear requirement that agencies have more detailed procedures in place. But Treasury's failure to develop and follow procedures to protect US persons is especially troubling given the more central role OIA has — which expanded in 2004 — in researching and designating terrorists, weapons proliferators, and drug kingpins.

> OIA makes intelligence actionable by supporting designations of terrorists, weapons proliferators, and drug traffickers and by providing information to support Treasury's outreach to foreign partners. OIA also serves as a unique and valuable source of information to the Intelligence Community (IC), providing economic analysis, intelligence analysis, and Treasury intelligence information reports to support the IC's needs.

As it is, such designations and the criminalization of US person actions that might violation sanctions imposed pursuant to such

designations are a black box largely devoid of due process (unless you're a rich Saudi business man). But Treasury's failure to establish procedures to protect US persons is especially troubling given how central these three topics — terrorists, weapons proliferation, and drugs — are in the intelligence communities overseas collection. This is where bulk collection happens. And yet any US persons suck up in the process and shared with Treasury have only ill-defined protections?

Treasury's role in spying on Americans may be little understood. But it is significant. And apparently they've been doing that spying without the required internal controls.

THE EMERGENCY EO 12333 FIX: SECTION 309

In a last minute amendment to the Intelligence Authorization, the House and Senate passed a new section basically imposing minimization procedures for EO 12333 or other intelligence collection not obtained by court order. (See Section 309)

> (3) Procedures.—
>
> (A) Application.—The procedures required by paragraph (1) shall apply to any intelligence collection activity not otherwise authorized by court order (including an order or certification issued by a court established under subsection (a) or (b) of section 103 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803)), subpoena, or similar legal process that is reasonably anticipated to result in the acquisition of a covered communication

> to or from a United States person and shall permit the acquisition, retention, and dissemination of covered communications subject to the limitation in subparagraph (B).
>
> (B) Limitation on retention.—A covered communication shall not be retained in excess of 5 years, unless—
>
> (i) the communication has been affirmatively determined, in whole or in part, to constitute foreign intelligence or counterintelligence or is necessary to understand or assess foreign intelligence or counterintelligence;
>
> (ii) the communication is reasonably believed to constitute evidence of a crime and is retained by a law enforcement agency;
>
> (iii) the communication is enciphered or reasonably believed to have a secret meaning;
>
> (iv) all parties to the communication are reasonably believed to be non-United States persons;
>
> (v) retention is necessary to protect against an imminent threat to human life, in which case both the nature of the threat and
> the information to be retained shall be reported to the congressional intelligence committees not later than 30 days after the
> date such retention is extended under this clause;
>
> (vi) retention is necessary for technical assurance or compliance purposes, including a court order or discovery obligation, in which case access to information retained for technical assurance or compliance purposes shall be reported to the congressional

> intelligence committees on an annual basis; or
>
> (vii) retention for a period in excess of 5 years is approved by the head of the element of the intelligence community responsible for such retention, based on a determination that retention is necessary to protect the national security of the United States, in which case the head of such element shall provide to the congressional intelligence committees a written certification describing—
> (I) the reasons extended retention is necessary to protect the national security of the United States; (II) the duration for which the head of the element is authorizing retention;
>
> (III) the particular information to be retained; and
>
> (IV) the measures the element ofthe intelligence community is taking toprotect the privacy interests of UnitedStates persons or persons locatedinside the United States.

The language seems to be related to — but more comprehensive than — language included in the RuppRoge bill earlier this year. That, in turn, seemed to arise out of concerns raised by PCLOB that some unnamed agencies had not revised their minimization procedures in the entire life of EO 12333.

Whereas that earlier passage had required what I'll call Reagan deadenders (since they haven't updated their procedures since him) to come up with procedures, this section effectively imposes minimization procedures similar to, though not identical, to what the NSA uses: 5 year retention except for a number of reporting requirements to Congress.

I suspect these are an improvement over whatever the deadenders have been using But as Justin

Amash wrote in an unsuccessful letter trying to get colleagues to oppose the intelligence authorization because of the late addition, the section provides affirmative basis for agencies to share US person communications whereas none had existed.

> Sec. 309 authorizes "the acquisition, retention, and dissemination" of nonpublic communications, including those to and from U.S. persons. The section contemplates that those private communications of Americans, obtained without a court order, may be transferred to domestic law enforcement for criminal investigations.
>
> To be clear, Sec. 309 provides the first statutory authority for the acquisition, retention, and dissemination of U.S. persons' private communications obtained without legal process such as a court order or a subpoena. The administration currently may conduct such surveillance under a claim of executive authority, such as E.O. 12333. However, Congress never has approved of using executive authority in that way to capture and use Americans' private telephone records, electronic communications, or cloud data.
>
> [snip]
>
> In exchange for the data retention requirements that the executive already follows, Sec. 309 provides a novel statutory basis for the executive branch's capture and use of Americans' private communications. The Senate inserted the provision into the intelligence reauthorization bill late last night.

Which raises the question of what the emergency was to have both houses of Congress push this through at the last minute? Back in March, after

all, RuppRoge was happy to let the agencies do this on normal legislative time.

I can think of several possibilities:

- The government is imminently going to have to explain some significant EO 12333 collection — perhaps in something like the Hassanshahi case or one of the terrorism cases explicitly challenging the use of EO 12333 data and it wants to create the appearance it is not a lawless dragnet (though the former was always described as metadata, not content)
- The government is facing new scrutiny on tools like Hemisphere, which the DOJ IG is now reviewing; if 27-year old data is owned by HIDTA rather than AT&T, I can see why it would cause problems (though again, except insofar as it includes things like location, that's metadata, not content)
- This is Dianne Feinstein's last ditch fix for the "trove" of US person content that Mark Udall described that John Carlin refused to treat under FISA
- This is part of the effort to get FBI to use EO 12333

> data (which may be related to the first bullet); these procedures are actually vastly better than FBI's see-no-evil-keep-all-data for up to 30 years approach, though the language of them doesn't seem tailored to the FBI

Or maybe this is meant to provide the patina of legality to some other dragnet we don't yet know about.

Still, I find it an interesting little emergency the intelligence committees seem to want to address.

ICREACH AND EO 12333

Because I need a hobby, I'm knee deep in tracking how EO 12333 got changed in 2008. Part of the impetus came from Congress, some members of which were furious that OLC had given the President authority to pixie dust EO 12333 in secret.

But the bigger impetus came from the Intelligence Community.

That's why this document — an NSA OGC memo on the sharing of raw SIGINT through database access released as part of ACLU's FOIA for EO 12333 documents — is so interesting.

It captures a July 12, 2007 discussion about whether or not NSA could share its data with other agencies by making it available in databases.

> You have asked us to conduct a legal review in order to set out the limits

> – and the rationale associated with the limits – on allowing personnel from other agencies access to NSA databases under the existing rules governing such access, and the advisability of changes to the Executive Order that would allow other agencies access to SIGINT databases.

While the memo adopts a cautious approach, recommending "case-by-case" access to SIGINT, it does embrace making SIGINT available by bringing Intelligence Committee partners into the production cycle (CIA and FBI both have people stationed at NSA), and finding ways to expand access to both phone and Internet metadata.

> There are substantial and well-grounded legal limits on NSA's ability to provide its partners and customers with access to raw SIGINT databases, both those that contain content and those that contain only metadata. Within those limits, NSA has lawfully expanded that access in two ways: with respect to content, we have expanded access by bringing IC partners within the SIGINT production chain in carefully defined circumstances. With respect to metadata, we have aggressively pushed telephony metadata to IC partners, and have plans in place to increase dramatically both the types and the completeness of the metadata we share.

Remember the timing of this: As The Intercept has reported, during precisely this period in 2007, NSA was implementing ICREACH – a sharing tool that would make metadata available to other agencies.

> "The ICREACH team delivered the first-ever wholesale sharing of communications metadata within the U.S. Intelligence Community," noted a top-secret memo dated December 2007. "This team

> began over two years ago with a basic concept compelled by the IC's increasing need for communications metadata and NSA's ability to collect, process and store vast amounts of communications metadata related to worldwide intelligence targets."

ICREACH is likely what the Deputy General Counsel mean when by the reference to "plans in place to increase dramatically both the types and completeness of the metadata we share."

But the memo helps to explain two more developments that happened in the year following this memo.

First, we know that starting in the fall, NSA started rolling out ways to chain through US person identities; Attorney General Michael Mukasey would sign off on that on January 3, 2008. The reasoning behind the change specifically involved making it easier to share metadata with CIA. That memo probably eliminated one of the problems with sharing US person phone records (not to mention Email records).

The memo provides interesting background to another change. While this memo did not advocate changing rules on sharing SIGINT under EO 12333, those rules nevertheless did change almost exactly a year after this memo came out. One of the significant changes to EO 12333 Bush implemented in July 2008 permitted the sharing of SIGINT content under Attorney General approved procedures.

> 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!

In other words, while the memo released strikes

the tone of conservatism, we know the limits it invoked (at least in the unredacted parts) were eliminated over the next year, even for SIGINT content.

FISCR USED AN OUTDATED VERSION OF EO 12333 TO RULE PROTECT AMERICA ACT LEGAL

If the documents relating to Yahoo's challenge of Protect America Act released last month are accurate reflections of the documents actually submitted to the FISC and FISCR, then the government submitted a misleading document on June 5, 2008 that was central to FISCR's ultimate ruling.

As I laid out here in 2009, FISCR relied on the the requirement in EO 12333 that the Attorney General determine there is probable cause a wiretapping technique used in the US is directed against a foreign power to judge the Protect America Act met probable cause requirements.

> The procedures incorporated through section 2.5 of Executive Order 12333, made applicable to the surveillances through the certifications and directives, serve to allay the probable cause concern.
>
> > The Attorney General hereby is delegated the power 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, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.
>
> 44 Fed. Reg. at 59,951 (emphasis supplied). Thus, in order for the government to act upon the certifications, the AG first had to make a determination that probable cause existed to believe that the targeted person is a foreign power or an agent of a foreign power. Moreover, this determination was not made in a vacuum. The AG's decision was informed by the contents of an application made pursuant to Department of Defense (DOD) regulations. See DOD, Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons, DOD 5240.1-R, Proc. 5, Pt. 2.C. (Dec. 1982).

Yahoo didn't buy this argument. It had a number of problems with it, notably that nothing prevented the government from changing Executive Orders.

> While Executive Order 12333 (if not repealed), provides some additional protections, it is still not enough.
>
> [snip]
>
> Thus, to the extent that it is even appropriate to examine the protections in the Executive Order that are not statutorily required, the scales of the reasonableness determination sway but do not tip towards reasonableness.

Yahoo made that argument on May 29, 2008.

Sadly, Yahoo appears not to have noticed the best argument that Courts shouldn't rely on EO 12333 because the President could always change it: Sheldon Whitehouse's revelation on December 7, 2007 (right in the middle of this litigation) that OLC had ruled the President could change it in secret and not note the change publicly. Whitehouse strongly suggested that the Executive in fact had changed EO 12333 without notice to accommodate its illegal wiretap program.

But the government appears to have intentionally withheld further evidence about how easily it could change EO 12333 — and in fact had, right in the middle of the litigation.

This is the copy of the Classified Annex to EO 12333 that (at least according to the ODNI release) the government submitted to FISCR in a classified appendix on June 5, 2008 (that is, after Yahoo had already argued that an EO, and the protections it affords, might change). It is a copy of the original Classified Appendix signed by Ed Meese in 1988.

As I have shown, Michael Hayden modified NSA/CSS Policy 1-23 on March 11, 2004, which includes and incorporates EO 12333, the day after the hospital confrontation. The content of the Classified Annex released in 2013 appears to be identical, in its unredacted bits, to the original as released in 1988 (see below for a list of the different things redacted in each version). So the actual content of what the government presented may (or may not be) a faithful representation of the Classified Appendix as it currently existed.

But the version of NSA/CSS Policy 1-23 released last year (starting at page 110) provides this modification history:

> This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998. The Associate Director for Policy endorsed an administrative update, effective 27

> December 2007 to make minor adjustments to this policy. This 29 May 2009 administrative update includes changes due to the FISA Amendments Act of 2008 and in core training requirements.

That is, Michael Hayden's March 11, 2004 modification of the Policy changed to the Directive as existed before 2 changes made under Clinton.

Just as importantly, the modification history reflects "an administrative update" making "minor adjustments to this policy" effective December 27, 2007 — a month and a half after this challenge started.

By presenting the original Classified Appendix — to which Hayden had apparently reverted in 2004 — rather than the up-to-date Policy, the government was presenting what they were currently using. But they hid the fact that they had made changes to it right in the middle of this litigation. A fact that would have made it clear that Courts can't rely on Executive Orders to protect the rights of Americans, especially when they include Classified Annexes hidden within Procedures.

In its language relying on EO 12333, FISCR specifically pointed to DOD 5240.1-R. The Classified Annex to EO 12333 is required under compliance with part of that that complies with the August 27, 2007 PAA compliance.

That is, this Classified Annex is a part of the Russian dolls of interlocking directives and orders that implement EO 12333.

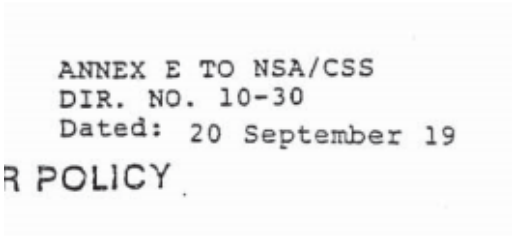
And they were changing, even as this litigation was moving forward.

Only, the government appears to have hidden that information from the FISCR.

Update: Clarified that NSA/CSS Policy 1-23 is what got changed.

Update: Hahaha. The copy of DOD 5240.1 R which

the government submitted on December 11, 2007, still bears the cover sheet labeling it as an Annex to NSA/CSS Directive 10-30. Which of course had been superseded in 2004.


ANNEX E TO NSA/CSS
DIR. NO. 10-30
Dated: 20 September 19
R POLICY

Note how they cut off the date to hide that it was 1990?

1988 version hides:

- Permission to intercept air and sea vessel radio communications to pursue international narcotics trade (Section 1)
- FBI's role in intercepting entirely foreign communication within the US (Definitions)
- The definitions of International Commercial Communications and National Diplomatic Communications
- The kinds of things that may be a selection in that definition
- The exclusion of diplomats from the definition of US person
- The inclusion of diplomatic and commercial communication among communications that may be targeted

- Parts of the permission to spy on foreign corporate subsidies in the US
- Parts of the paragraph permitting 72 hours of SIGINT upon entry into the US
- A paragraph permitting surveillance on communications (?) with terminal in the US targeted at foreigners
- Parts of the paragraph limiting surveillance of voice and fax unless usedexclusively by a foreign power
- All of paragraph g in targeting
- All of paragraph B permitting the collection of international communications of non-resident aliens in the US
- The paragraph permitting interception of foreign interception within the US, with FISA approval

The 2004/2009 version hides:

- The definition of "transiting communications"
- Different parts of permission to spy on foreign corporate subsidies in the US
- Different parts of the

paragraph permitting 72 hours of SIGINT upon entry into the US
- Different parts of the paragraph limiting surveillance of voice and fax unless used exclusively by a foreign power

---

THE OTHER BLIND SPOT IN NSA'S EO 12333 PRIVACY REPORT: RESEARCH

Yesterday, I laid out the biggest reason the NSA Privacy Officer's report on EO 12333 was useless: she excluded most of NSA's EO 12333 collection — its temporary bulk collection done to feed XKeyscore and its more permanent bulk collection done to hunt terrorists and most other NSA targets — from her report. Instead, Privacy Officer Rebecca Richards' report only covered a very limited part of NSA's EO 12333 spying, that targeting people like Angela Merkel.

But I wanted to circle back and note two other things she did which I find telling.

First, note what Richards didn't do.
The standard by which she measured NSA's privacy efforts is a NIST standard called Fair Information Practice Principles, which include the following:

- Transparency
- Individual Participation
- Purpose Specification

- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

She dismisses the first two because NSA is a spook organization.

> Because NSA has a national security mission, the principles of *Transparency* and *Individual Participation* are not implemented in the same manner they are in organizations with a more public facing mission.

In the process, she overstates how assiduously NSA lets Congress or DOJ review EO 12333 activities.

For the rest, however, Richards doesn't — as she should have — assess NSA's compliance with each category. Had she done so, she would have had to admit that PCLOB found NSA's retention under the Foreign Intelligence purpose to be far too broad, putting NSA in violation of Purpose Specification; she would have had to admit that NSA gets around Use Limitation with broad permissions to create technical databases and keep all encrypted communications; she would have had to admit that of NSA's violations, 9% constitute a willful refusal to follow Standard Operating Procedures, a stat that would seem to belie her Accountability claims.

Rather than assessing whether NSA complies with these principles, then, Richards simply checks them off at the end of each of several sections on the SIGINT Production Cycle.

> ACQUIRE, Targeting: "The existing civil liberties and privacy protections fall into the following FIPPs: Transparency (to overseers), Purpose Specification, and Accountability and Auditing."
>
> ACQUIRE, Collection and Processing: "The

> existing civil liberties and privacy protections fall into three FIPPs categories: Data Minimization, Purpose Specification and Accounting and Auditing."
>
> ANALYZE: "These existing civil liberties and privacy protections fall into the following FIPPs: Transparency (to overseers), Purpose Specification, Data Minimization, and Accountability and Auditing."
>
> RETAIN: "These existing civil liberties and privacy protections fall into the following two FIPPs: Data Minimization, and Security."
>
> DISSEMINATE: "The existing civil liberties and privacy protections fall into the following FIPPs: Use Limitations, Data Minimization, and Accountability and Auditing."

Then, having laid out how the NSA does some things that fall into some of these boxes at each step of the SIGINT process, she concludes,

> CLPO documented NSA's multiple activities that provide civil liberties and privacy protections for six of the eight FIPPs that are underpinned by its management activities, documented compliance program, and investments in people, training, tools, and technology.

Fact check! Even buying her claim that checking the box for some of these things at each step of the process is adequate to assessing whether it fulfills FIPP, note that she hasn't presented any evidence NSA meets NIST's "Data Quality and Integrity" claim (though that may just be sloppiness on her part, a further testament to the worthlessness of this review).

But there's another huge problem with this approach.

By fulfilling her privacy review by checking the boxes for the SIGINT Production Cycle (just for the targeted stuff, remember, not for the bulk of what NSA does), Richards leaves out all the other things the NSA does with the world's data. Most notably, she doesn't consider the privacy impacts of NSA's research — what is called SIGDEV — which NSA and its partners do with live data. Some of the most aggressive programs revealed by Edward Snowden's leaks — especially to support their hacking and infiltration activities — were SIGDEV presentations. Even on FISA programs, SIGDEV is subjected to nowhere near the amount of auditing that straight analysis is.

And the most significant known privacy breach in recent years involved the apparent co-mingling of 3,000 files worth of raw Section 215 phone dragnet data with Stellar Wind data on a research server. NSA destroyed it all before anyone could figure out what it was doing there, how it got there, or what scope "3,000" files entailed.

> In my **obsessions** with the poor oversight over the phone dragnet techs, I have pointed to **this description** several times.
>
> > As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to

> > document why certain contact chaining rules were created. In addition to the BR work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata.

The NSA just finds raw data mingling with data from the President's illegal program. And that's all the explanation we get for why!

Well, PCLOB **provides** more explanation for why we don't know what happened with that data.

> > In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a

> > migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.
>
> This is actually PCLOB being more solicitous in other parts of the report. After all, it's not just that there was a 5 year data retention limit on this data, there was also a mandate that techs destroy data once they're done fiddling with it. So this is a double violation.
>
> And yet NSA's response to finding raw data sitting around places is to destroy it, making it all the more difficult to understand what went on with it?

Richards may be referring to this kind of oopsie when she talks about "spillage" being a risk related to retention.

> The civil liberties and privacy risks related to retention are that NSA (1) may possibly retain data that it is no longer authorized to retain; (2) may possibly fail to completely remove data the Agency was not authorized to acquire; and (3) may potentially lose data because of "spillage," improper intentional disclosure, or malicious exfiltration.

But nowhere does she consider the privacy implications of having a "technical database"

data retention exemption even for Section 702 data, and then subjecting that raw data to the most exotic projects NSA's research staff can think of.

And given that she elsewhere relies on President Obama's PPD-28 as if it did anything to protect privacy, note that that policy specifically exempts SIGDEV from its limits.

> Unless otherwise specified, this directive shall apply to signals intelligence activities conducted in order to collect communications or information about communications, except that it shall not apply to signals intelligence activities undertaken to test or develop signals intelligence capabilities.

We know NSA doesn't abide by privacy rules for its research function. Not only does that mean a lot of probably legitimate research evades scrutiny, it also creates a space where NSA can conduct spying, in the name of research, that wouldn't fulfill any of these privacy protections.

That's a glaring privacy risk. One she chooses not to mention at all in her report.

NSA'S PRIVACY OFFICER EXEMPTS MAJORITY OF NSA SPYING FROM HER REPORT ON EO 12333 COLLECTION

NSA's Director of Civil Liberties and Privacy, Rebecca Richards, has another report out, this

time on “Civil Liberties and Privacy Protections” provided in the Agency’s EO 12333 programs. As with her previous report on Section 702, this one is almost useless from a reporting standpoint.

The reason why it is so useless is worth noting, however.

Richards describes the scope of her report this way:

> This report examines (1) NSA’s Management Activities that are generally applied throughout the Agency and (2) Mission Safeguards within the SIGINT mission when specifically conducting targeted3 SIGINT activities under E.O. 12333.
>
> 3 In the context of this paper, the phrase “targeted SIGINT activities” does not include “bulk” collection as defined in Presidential Policy Directive (PPD)-28. Footnote 5 states, in part, “References to signals intelligence collected in ‘bulk’ mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).”

Richards neglects to mention the most important details from PPD-28 on bulk collection: when collection in “bulk” is permitted.

> Locating new or emerging threats and other vital national security information is difficult, as such information is often hidden within the large and complex system of modern global communications. The United States must consequently collect signals intelligence in bulk5 in certain circumstances in order to identify these threats. Routine communications and

> communications of national security interest increasingly transit the same networks, however, and the collection of signals intelligence in bulk may consequently result in the collection of information about persons whose activities are not of foreign intelligence or counterintelligence value. The United States will therefore impose new limits on its use of signals intelligence collected in bulk. These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside.
>
> In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section. In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section.

> 5 The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection. References to signals intelligence collected in "bulk" mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.).

The NSA collects in "bulk" (that is, "everything"), temporarily, to facilitate targeted collection. This refers to the 3-5 day retention of all content and 30 day retention of all metadata from some switches so XKeyscore can sort through it to figure out what to keep.

And the NSA also collects in "bulk" (that is, "everything") to hunt for the following kinds of targets:

- Spies
- Terrorists
- Weapons proliferators
- Hackers and other cybersecurity threats
- Threats to armed forces
- Transnational criminals (which includes drug cartels as well as other organized crime)

Of course, when NSA collects in "bulk" (that is, "everything") to hunt these targets, it also collects on completely innocent people because, well, it has collected *everything*.

So at the start of a 17-page report on how many "civil liberties and privacy protections" the NSA uses with its EO 12333 collection, NSA's Privacy Officer starts by saying what she's about to report doesn't apply to NSA's

temporary collection of *everything* to sort through it, nor does it apply to its more permanent collection of *everything* to hunt for spies, terrorists, weapons proliferators, hackers, and drug bosses.

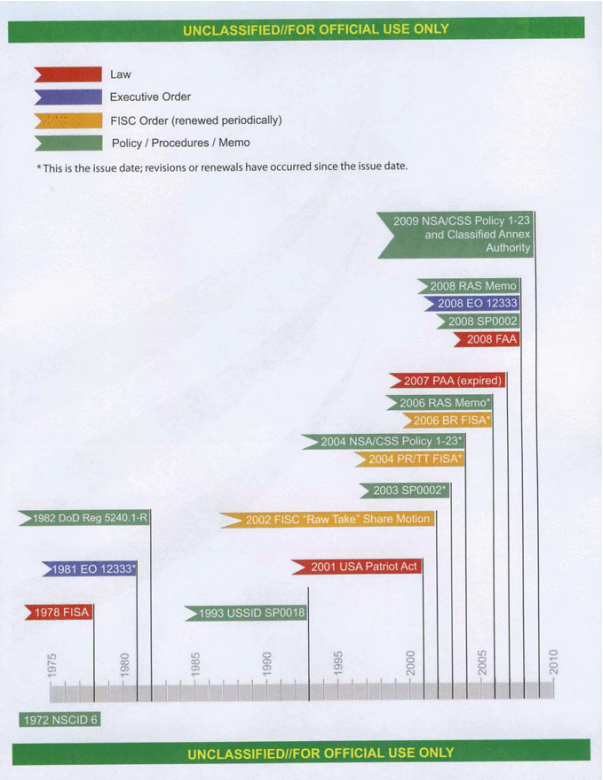
That is, the "civil liberties and privacy protections" Richards describe don't apply to the the great majority of what NSA does. And these "civil liberties and privacy protections" don't apply until after NSA has collected everything and decided, over the course of 5 days, whether it wants to keep it and in some places, kept everything to be able to hunt a range of targets.

This actually shows up in Richards' report, subtly, at times, as when she emphasizes that her entire "ACQUIRE" explanation focuses on "targeted SIGINT collection." What that means, of course, is that process, where collecting only takes place after an NSA analyst has targeted the collection? It doesn't happen in the majority of cases.

Once you collect and sort through *everything*, does it really make sense to claim you're providing civil liberties and privacy protections?

MISSING FROM THE EO 12333 DISCUSSION: ITS CLASSIFIED ANNEX MICHAEL HAYDEN REVISED ON MARCH 11, 2004

I recommend this ArsTechnica background piece on EO 12333. It describes how Ronnie Reagan issued EO 12333 to loosen the intelligence rules imposed by Jimmy Carter (with links to key historical documents). It includes interviews with the NSA whistleblowers describing how George Bush authorized the collection of telecom data from circuits focused on the US under the guise of EO 12333, calling the bulk of the US person data collected "incidental." And it describes how Bush and Obama have continued using EO 12333 as a loophole to obtain US person data.



But there's a key part of the story Ars misses, which I started to lay out here. As this graphic notes, the NSA is governed by a set of interlocking authorities and laws. The precedence of those authorities and laws is not terribly clear — and NSA's own training programs don't make them any more clear. Bush's revision to EO 12333 played on that interlocking confusion.

Perhaps most alarming, however, the NSA continued to use a classified annex to EO 123333 written by Michael Hayden the day he reauthorized the illegal wiretap program at least until recent years — and possibly still. And that classified annex asserts an authority to wiretap Americans on the Attorney General's

authorization for periods of up to 90 days, and wiretap "about" collection based solely on NSA Director authority.

Among the documents released to ACLU and EFF via FOIA was an undated "Core Intelligence Oversight Training" program that consists of nothing more than printouts of the authorities governing NSA activities (as I noted in this post, with one exception, the NSA training programs we've seen are unbelievably horrible from a training efficacy standpoint). It includes, in part, EO 12333, DOD 5240.1-R, and NSA/CSS Policy 1-23 (that is, several of the authorities NSA considers among its signature authorities). As part of a 2009 issuance of the latter document (starting on page 110), the training documents also include the classified annex to EO 12333 (starting on page 118). And although both documents are part of that 2009 issuance (which incorporated language reflecting the FISA Amendments Act), they are dated March 11, 2004 — the day after the hospital confrontation, when the Bush Administration continued its illegal wiretap program without DOJ sanction — and signed by then DIRNSA Michael Hayden.

That is, as part of the FOIA response to ACLU and EFF, DOJ revealed how it was secretly applying EO 12333 at least as recently as 2009.

And that secret application of EO 12333 includes two provisions that illustrate how the government was abusing EO 12333, even in the face of revisions to FISA. They include provisions permitting the wiretapping of Americans for 90-day periods based on AG certification, and the wiretapping of "about" communications for apparently unlimited periods based on DIRNSA certification. (see page 123)

Here's the AG-certified 90-day provision.

> (4) with specific prior approval by the Attorney General based on a finding by the Attorney General that there is probable cause to believe the United States person is an agent of a foreign

> power and that the purpose of the interception or selection is to collect significant foreign intelligence. Such approvals shall be limited to a period of time not to exceed ninety days for individuals and one year for entities.

The illegal wiretap program operated on 45-day authorizations from the AG. We don't know from this what changes Hayden made the day after DOJ refused to reauthorize the program, but if Hayden changed it to 90 days, it effectively extended the previous authorization for another period.

And here's the part of the "about" collection that is not redacted.

> (b) Communications of, or concerning (1) [redacted] of a foreign power, or powers, as defined in Section 101 (a) (1) – (3) of FISA or (2) [redacted] may be intercepted intentionally, or selected deliberately (through the use of a selection term or otherwise), upon certification in writing by the Director, NSA to the Attorney General. Such certification shall take the form of the Certification Notice appended thereto. An information copy shall be forwarded to the Deputy Secretary of Defense. Collection may commence upon the Director, NSA's certification. In addition, the Director, NSA shall advise the Attorney General and the Deputy Secretary of Defense on an annual basis of all such collection.

This "about" collection is ostensibly not targeted at US persons, but we know from the problems NSA confessed to in the 2011 702 upstream program that "about" collection ensnares a good deal of US person data — so much so NSA could not or would not count it when John Bates asked them to.

At least 5 years after the hospital confrontation and 2 years after Congress purportedly passed laws addressing the underlying issue, NSA's own secret interpretation of how it implemented EO 12333 said it could continue to do the same domestic wiretapping, authorized by either the AG (for wiretapping targeting US persons for up to 90-day periods) or the DIRNSA (for wiretapping targeting communications "about" foreign powers).

The Bush Administration explicitly argued it was not bound by FISA — the law that should govern both these activities. Did the Obama Administration continue that policy?

October 20, 2014 update: As far as I can tell, Hayden's version of the classified annex was identical to the annex as issued in 1988, released here (there are different redactions in the release). Given this language, it appears to reflect a reversion to the earlier policy, overriding Clinton-era changes.

> This Policy 1-23 supersedes Directive 10-30, dated 20 September 1990, and Change One thereto, dated June 1998. The Associate Director for Policy endorsed an administrative update, effective 27 December 2007 to make minor adjustments to this policy. This 29 May 2009 administrative update includes changes due to the FISA Amendments Act of 2008 and in core training requirements.

THE TRUTH MISSING FROM ALEXANDER

JOEL'S "TRUTH" ABOUT EO 12333

Over at Salon, I've got a piece responding to Office of Director of National Intelligence Civil Liberties Officer Alexander Joel's column purporting to describe the "truth" about EO 12333.

Click through to see this part of my argument:

- Joel resorts to the tired old "target" jargon
- Joel points to PPD 28, which rather than supporting his point, actually shows how broadly the NSA uses bulk collection and therefore how meaningless that "target" jargon is
- Joel doesn't address one of John Napier Tye's points — that current technology allows the NSA to collect US person data overseas
- We know they're doing that in the SPCMA — the Internet dragnet authority conducted on Internet data collected overseas

But it's Joel's claim about oversight I find most problematic.

> Oversight is extensive and multi-layered. Executive branch oversight is provided internally at the NSA and by both the Department of Defense and the Office of the DNI by agency inspectors general, general counsels, compliance officers and privacy officers (including

> my office and the NSA's new Civil Liberties and Privacy Office). The Department of Justice also provides oversight, as do the Privacy and Civil Liberties Oversight Board and the president's Intelligence Oversight Board. In addition, Congress has the power to oversee, authorize and fund these activities.

As I note in my piece, really what we have is single branch oversight. And that's not going to prevent abusive spying.

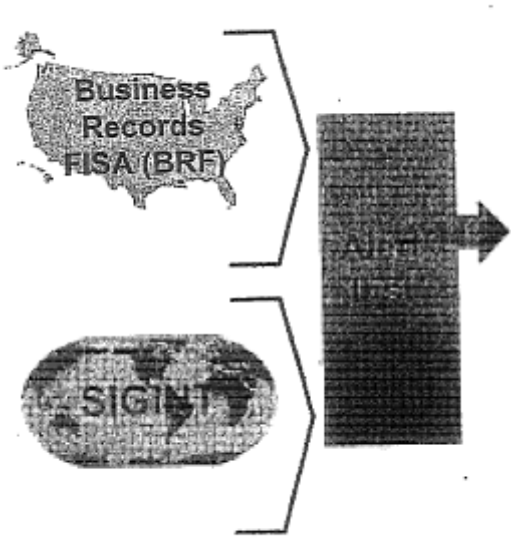
> Joel's claim,"Oversight [of EO 12333 collection] is extensive and multi-layered," rings hollow. He lists 4 oversight positions at 3 Executive branch agencies, then points to 3 more Executive branch agencies he claims have a role. Having the Executive oversee the Executive spying on Americans poses precisely the kind of threat to our democracy Tye raised.
>
> Then Joel claims, "Congress has the power to oversee, authorize and fund these activities." Of course, that's different from Congress actually using that power. Moreover, the record suggests Congress may not currently have the power to do anything but defund such spying, assuming they even know about it. Senate Intelligence Committee Chair Dianne Feinstein admitted last August that her committee doesn't receive adequate information on EO 12333 collection. Joel's boss, James Clapper, refused to answer a question from Senator Amy Klobuchar on EO 12333 violations in a hearing in October. And when Senator Mark Udall suggested a "vast trove" of Americans' communications collected overseas should be provided the protections laid out in FISA, Assistant Attorney General John Carlin explained the National Security

> Division — the part of DOJ he oversees, which has a central role in oversight under FISA — would not have a role in that case because the collection occurred under EO 12333.
>
> In his column, Joel makes no mention of the third branch of government: the Courts. That's because, as ACLU's Patrick Toomey laid out last week, the government doesn't give defendants any notice if their prosecutions arise from data collected under EO 12333. Criminal prosecutions are where some of the most important oversight on Executive branch spying takes place. By exempting EO 12333 from any such notice, then, the government is bypassing another critical check on potentially abusive spying.
>
> Back in 1978, our government decided that both Congress and the courts should have a role when the Executive branch spied on Americans. That was the entire premise behind the FISA law. But by moving more and more of its spying overseas, the government can and — apparently, at least to a limited extent — *is* bypassing the oversight accorded through three branches of government.

FISA was written in 1978, before it became so easy to spy on Americans' domestic communications overseas. FISA Amendments Act partly addressed the new technological reality — by giving the Executive permission to spy on foreigners domestically. But it provided inadequate protections — Sections 703-5 — in return. Those measures, requiring a Court order for targeting Americans who are themselves overseas (but not for targeting Americans' data that transits overseas), simply don't do enough to prevent the government from using this new technological reality from spying on Americans.

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 EO 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 SIGNIT (that is, EO 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 EO 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 Articulable 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.

EO 12333 THREATENS OUR DEMOCRACY

Among the many posts I've written about Executive Order 12333 — the order that authorizes all non-domestic spying — includes this post, where I noted that proposed changes to NSA's phone dragnet won't affect programs authorized by EO 12333.

> Obama was speaking only about NSA's treatment of Section 215 metadata, not the data — which includes a great amount of US person data — collected under Executive Order 12333.
>
> [snip]
>
> Section 215 metadata has different and significantly higher protections than EO 12333 phone metadata because of specific minimization procedures imposed by the FISC (arguably, **the program doesn't even meet the minimization procedure** requirements mandated by the law). We've seen the implications of that, for example, when the NSA **responded** to being caught watch-listing 3,000 US persons without extending First Amendment protection not by stopping that tracking, but simply cutting off the watch-list's ability to draw on Section 215 data.
>
> Basically, the way NSA treats data collected under FISC-overseen programs (including both Section 215 and FISA Amendments Act) is to throw the data in with data collected under EO 12333, but add query screens tied to the more strict FISC-regulations governing production under it.
>
> [snip]
>
> NSA's spokeswoman will say over and over that "everyday" or "ordinary" Americans

> don't have to worry about their favorite software being sucked up by NSA. But to the extent that collection happens under EO 12333, they have relatively little protection.

That's precisely the point made in an important op-ed by the State Department's former Internet freedom chief, John Napier Tye, who had access to data from EO 12333 collection.

> Bulk data collection that occurs inside the United States contains built-in protections for U.S. persons, defined as U.S. citizens, permanent residents and companies. Such collection must be authorized by statute and is subject to oversight from Congress and the Foreign Intelligence Surveillance Court. The statutes set a high bar for collecting the content of communications by U.S. persons. For example, Section 215 permits the bulk collection only of U.S. telephone metadata — lists of incoming and outgoing phone numbers — but not audio of the calls.
>
> Executive Order 12333 contains no such protections for U.S. persons if the collection occurs outside U.S. borders.
>
> [snip]
>
> Unlike Section 215, the executive order authorizes collection of the content of communications, not just metadata, even for U.S. persons. Such persons cannot be individually targeted under 12333 without a court order. However, if the contents of a U.S. person's communications are "incidentally" collected (an NSA term of art) in the course of a lawful overseas foreign intelligence investigation, then Section 2.3(c) of the executive order explicitly authorizes their retention. It does not require that the affected U.S. persons

> be suspected of wrongdoing and places no limits on the volume of communications by U.S. persons that may be collected and retained.

Tye reveals that a document the White House provided to Congress said it had no intention of limiting back door searches of EO 12333 collected data because it would require too many changes to existing programs.

> In that document, the White House stated that adoption of Recommendation 12 [which would requiring purging US person data] would require "significant changes" to current practice under Executive Order 12333 and indicated that it had no plans to make such changes.

And Tye implies that NSA is using EO 12333 to conduct the Internet dragnet.

> All of this calls into question some recent administration statements. Gen. Keith Alexander, a former NSA director, has said publicly that for years the NSA maintained a U.S. person e-mail metadata program similar to the Section 215 telephone metadata program. And he has maintained that the e-mail program was terminated in 2011 because "we thought we could better protect civil liberties and privacy by doing away with it."Note, however, that Alexander never said that the NSA stopped collecting such data — merely that the agency was no longer using the Patriot Act to do so. I suggest that Americans should dig deeper.

I have made repeatedly covered SPCMA, the EO 12333 authorized Internet dragnet, which the government rolled out just as it was shutting down its PATRIOT-authorized Internet dragnet.

Because you've been reading me, you already knew what most others are only discovering because of this op-ed.

The most important point Tye made — it's one I've made too, but it can't be said enough — is this:

> The [Executive] order as used today threatens our democracy.

There is almost no oversight over this — and when Mark Udall suggested DOJ should exercise more of a role, the AAG for National Security showed no interest. This is the executive choosing to spy on Americans outside of all oversight.

That's a threat to our democracy.