SURVEILLANCE REFORM CAN NO LONGER IGNORE EO 12333

Yesterday, a bunch of civil liberties groups issued a letter calling for FISA 702 reform as part of the Section 215 reauthorization this year. I agree that the reauthorization this year should address the problems with 702 that weren't addressed last year, though even on FISA, the letter doesn't go far enough. DOJ IG will soon issue a report partly addressing the Carter Page FISA application, and that will provide an opportunity to push to make reforms to traditional (individual) FISA, such as making it clear that some defendants must get to review the underlying affidavit. Similarly, it doesn't make sense reforming Section 215's subpoena function without, at the same time, reforming the subpoena authority that DEA uses for a similar dragnet that undergoes far less oversight, particularly given that Bill Barr is the guy who first authorized that DEA dragnet in his first go-around as authoritarian Attorney General.

But it's also the case that the surveillance community could — and arguably has an opportunity to — address EO 12333 as well.

The Executive branch has been exploiting the tension between EO 12333 (foreign surveillance that, because it is "foreign," is conducted under the exclusive authority of Article II) and FISA ("domestic" surveillance overseen by the FISA court) since Dick Cheney launched Stellar Wind on bogus claims the collection on foreign targets in the US amounted to "foreign" surveillance. From 2004 to 2008, Congress moved parts of that under FISA. But at several points since, the government has reacted to FISA restrictions by moving their surveillance under EO 12333, most notably when it moved much of its collection of Internet metadata under EO 12333 in 2012.

Unfortunately, most of the surveillance community and reporters covering such issues have been woefully unaware of even the limited public disclosures on EO 12333 surveillance (which for a time was branded as SPCMA). That made activism around Section 215 far less effective, as few people understood that Section 215 data was and remains just a small part of a larger, duplicative dragnet, and a lot of the claims made about the need for USA Freedom Act didn't account for precisely what role the Section 215 dragnet played in the larger whole.

As one of its last acts, the Obama Administration institutionalized EO 12333 sharing across intelligence agencies, formalizing what Dick Cheney had been aiming for all along, just before Donald Trump took over. At least as soon as that happened, the FBI (and other agencies, including but not limited to CIA) obtained a source of *content* that paralleled (and like the metadata dragnet, surely is significantly duplicative with) Section 702 collection.

That means the Section 702 opinion released last week discusses querying methods that may also be applied, in the same systems, to EO 12333 data. Indeed, one aspect of the querying procedures FBI finally adopted — that queries limited "such that it cannot retrieve unminimized section 702-acquired information" — is the kind of setting that NSA used to re-run queries that returned FISA information so as to return, instead, only EO 12333 data that could be shared under different rules with less oversight. Furthermore, the regime set up under EO 12333, which already includes squishy language about queries "for the purpose of targeting" a US person (suggesting other purposes are permissible), has the same kind of internal approval process that the government wanted to adopt with 702.

If FBI is querying both 702 and EO 12333 raw content in the same queries, it means the standards laid out by James Boasberg in his

opinion should apply. Notably, Boasberg wrote at some length about what constituted "reasonable" procedures to govern querying, and under a balancing analysis, found that the procedures in place did not comply with the Fourth Amendment.

> Whether the balance of interests ultimately tips in favor of finding the procedures to be inconsistent with the Fourth Amendment is a close question. Reasonableness under the Fourth Amendment does not require perfection. See In Re Directives, 551 F.3d at J 015 ("the fact that there is some potential for error is not a sufficient reason to invalidate" surveillances as unreasonable under the Fourth Amendment). Nonetheless, if "the protections that are in place for individual privacy interests are … insufficient to alleviate the risks of government error and abuse, the scales will tip toward a finding of unconstitutionality." kl at 1012. Here, there are demonstrated risks of serious error and abuse, and the Court has found the government's procedures do not sufficiently guard against that risk, for reasons explained above in the discussion of statutory minimization requirements.

By contrast, under the EO 12333 procedures, the only reasonableness review takes place when NSA decides whether to share its SIGINT, which doesn't include risk of error and abuse.

> Reasonableness. Whether approving the request is reasonable in light of all the circumstances known at the time of the evaluation of the request, including but not limited to:
>
> [snip]
>
> e. (U) The likelihood that sensitive U.S. person information (USPI) will be

> found in the information and, if known, the amount of such information;
>
> f. (U) The potential for substantial harm, embarrassment, inconvenience, or unfairness to U.S. persons if the USPI is improperly used or disclosed;

And that's *with* the additional minimization procedures under 702 that are stronger than the dissemination rules under the EO 12333 rules.

There are limits to this. Boasberg based his Fourth Amendment review in statutory considerations, statute that doesn't yet exist with 12333. He did not determine that the act of querying, by itself, warranted Fourth Amendment protection (though the amici pushed him to do so).

But that shouldn't stop Congress from requiring that FBI adhere to the same practices of querying with EO 12333 collected data as it does with Section 702 collected data, which would in turn limit the value, to FBI, of engaging in surveillance arbitrage by doing things under EO 12333 that it couldn't do under 702.

EO 12333 SHARING WILL LIKELY EXPOSE SECURITY RESEARCHERS EVEN MORE VIA BACK DOOR SEARCHES

At Motherboard, I have piece arguing that the best way to try to understand the Marcus Hutchins (MalwareTech) case is not from what we see in his indictment for authoring code that appears in a piece of Kronos malware sold in

2015. Instead, we should consider why Hutchins would look different to the FBI in 2016 (when the government didn't arrest him while he was in Las Vegas) and 2017 (when they did). In 2016, he'd look like a bit player in a minor dark market purchase made in 2015. In 2017, he might look like a guy who had his finger on the WannaCry malware, but also whose purported product, Kronos, had been incorporated into a really powerful bot he had long closely tracked, Kelihos.

> Hutchins' name shows up in chats obtained in an investigation in some other district. Just one alias for Hutchins—his widely known "MalwareTech"—is mentioned in the indictment. None of the four or more aliases Hutchins may have used, mostly while still a minor, was included in the indictment, as those aliases likely would have been if the case in chief relied upon evidence under that alias.
>
> Presuming the government's collection of both sets of chat logs predates the WannaCry outbreak, if the FBI searched on Hutchins after he sinkholed the ransomware, both sets of chat logs would come up. Indeed, so would any other chat logs or—for example—email communications collected under Section 702 from providers like Yahoo, Google, and Apple, business records from which are included in the discovery to be provided in Hutchins' case in FBI's possession at that time. Indeed, such data would come up even if they showed no evidence of guilt on the part of Hutchins, but which might interest or alarm FBI investigators.
>
> There is another known investigation that might elicit real concern (or interest) at the FBI if Hutchins's name showed up in its internal Google search: the investigation into the Kelihos

> botnet, for which the government obtained a Rule 41 hacking warrant in Alaska on April 10 and announced the indictment of Russian Pyotr Levashov in Connecticut on April 21. Eleven lines describing the investigation in the affidavit for the hacking warrant remain redacted. In both its announcement of his arrest and in the complaint against Levashov for operating the Kelihos botnet, the government describes the Kelihos botnet loading "a malicious Word document designed to infect the computer with the Kronos banking Trojan."
>
> Hutchins has tracked the Kelihos botnet for years—he even attributes his job to that effort. Before his arrest and for a period that extended after Levashov's arrest, Hutchins ran a Kelihos tracker, though it has gone dead since his arrest. In other words, the government believes a later version of the malware it accuses Hutchins of having a hand in writing was, up until the months before the WannaCry outbreak—being deployed by a botnet he closely tracked.
>
> There are a number of other online discussions Hutchins might have participated in that would come up in an FBI search (again, even putting aside more dated activity from when he was a teenager). Notably, the attack on two separate fundraisers for his legal defense by credit card fraudsters suggests that corner of the criminal world doesn't want Hutchins to mount an aggressive defense.
>
> All of which is to say that the FBI is seeing a picture of Hutchins that is vastly different than the public is seeing from either just the indictment and known facts about Kronos, or even open source investigations into

> Hutchins' past activity online.

To understand why Hutchins was arrested in 2017 but not in 2016, I argue, you need to understand what a back door search conducted on him in May would look like in connection with the WannaCry malware, not what the Kronos malware looks like as a risk to the US (it's not a big one).

I also note, however, that in addition to the things FBI admitted they searched on during their FBI Google searches — Customs and Border Protection data, foreign intelligence reports, FBI's own case files, and FISA data (both traditional and 702) — there's something new in that pot: data collected under EO 12333 shared under January's new sharing procedures.

That data is likely to expose a lot more security researchers for behavior that looks incriminating. That's because FBI is almost certainly prioritizing asking NSA to share criminal hacker forums — where security researchers may interact with people they're trying to defend against in ways that can look suspicious if reviewed out of context. That's true, first of all, because many of those forums (and other dark web sites) are overseas, and so are more accessible to NSA collection. The crimes those forums facilitate definitely impact US victims. But criminal hacking data — as distinct from hacking data tied to a group that the government has argued is sponsored by a nation-state — is also less available via Section 702 collection, which as far as we know still limits cybersecurity collection to the Foreign Government certificate.

If I were the FBI I would have used the new rules to obtain vast swaths of data sitting in NSA's coffers to facilitate cybersecurity investigations.

So among the NSA-collected data we should expect FBI newly obtained in raw form in January is that from criminal hacking forums. Indeed, new dark web collection may have facilitated FBI's

rather impressive global bust of several dark web marketing sites this year. (The sharing also means FBI will no longer have to go the same lengths to launder such data it obtains targeting kiddie porn, which it appears to have done in the PlayPen case.)

As I think is clear, such data will be invaluable for FBI as it continues to fight online crime that operates internationally. But because back door searches happen out of context, at a time when the FBI may not really understand what it is looking at, it also risks exposing security researchers in new ways to FBI's scrutiny.

THE IRONIES OF THE EO 12333 SHARING EXPANSION FOR OBAMA AND TRUMP

There are a lot of ironies in the EO 12333 sharing procedures signed earlier this month. Perhaps most significant of all, they should put a lot more counterintelligence information on Trump's ties with Russia in the hands of the FBI.

12333 INFO SHARING WORKING THREAD

This is my very weedy analysis of the new sharing procedures for EO 12333. I'll do a

subsequent post that narrativizes these changes.

ON THE COMING SHOWDOWN OVER PROMISCUOUS SHARING OF EO 12333 DATA

A number of outlets are reporting that Ted Lieu and Blake Farenthold have written a letter to NSA Director Mike Rogers urging him not to implement the new data sharing effort reported by Charlie Savage back in February. While I'm happy they wrote the letter, they use a dubious strategy in it: they suggest their authority to intervene comes from Congress having "granted" NSA authority to conduct warrantless collection of data.

> Congress granted the NSA extraordinary authority to conduct warrantless collection of communications and other data.2
>
> 2 See Foreign Intelligence Surveillance Act and the Patriot Act.

As an initial matter, they've sent this letter to a guy who's not in the chain of approval for the change. Defense Secretary Ash Carter and Attorney General Loretta Lynch will have to sign off on the procedures developed by Director of National Intelligence James Clapper; they might consult with Rogers (if he isn't the one driving the change), but he's out of the loop in terms of implementing the decision.

Furthermore, the Congressionally granted authority to conduct warrantless surveillance under FISA has nothing to do with the authority under which NSA collects this data, EO 12333. In

his story, Savage makes clear that the change relies on the [what he called "little-noticed," which is how he often describes stuff reported here years earlier] changes Bush implemented in the wake of passage of FISA Amendments Act. As I noted in 2014,

> 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.

What Bush did just as he finished moving most of Stellar Wind over to FISA authorities, was to make it permissible to share EO 12333 data with other intelligence agencies under the same kind of DNI/AG/DOD approval process already in place

for surveillance. They've already been using this change (though as I note, in some ways the new version of EO 12333 made FAA sharing even more permissive than EO 12333 sharing). And Savage's article describes that they've intended to roll out this further expansion since Obama's first term.

> Obama administration has been quietly developing a framework for how to carry it out since taking office in 2009.
>
> [snip]
>
> Intelligence officials began working in 2009 on how the technical system and rules would work, Mr. Litt said, eventually consulting the Defense and Justice Departments. This month, the administration briefed the Privacy and Civil Liberties Oversight Board, an independent five-member watchdog panel, seeking input. Before they go into effect, they must be approved by James R. Clapper, the intelligence director; Loretta E. Lynch, the attorney general; and Ashton B. Carter, the defense secretary.
>
> "We would like it to be completed sooner rather than later," Mr. Litt said. "Our expectation is months rather than weeks or years."

All of which is to say that if Lieu and Farenthold want to stop this, they're going to have to buckle down and prepare for a fight over separation of powers, because Congress has had limited success (the most notable successes being imposition of FAA 703-705 and Section 309 of last year's intelligence authorization) in imposing limits on EO 12333 collection. Indeed, Section 309 is the weak protection Dianne Feinstein and Mark Udall were able to get for activities they thought should be covered under FAA.

Two more points. First, I suspect such expanded

sharing is already going on between NSA and DEA. I've heard RUMINT that DEA has actually been getting far *more* data since shutting down their own dragnets in 2013. The sharing of "international" narcotics trade data has been baked into EO 12333 from the very start. So it would be unsurprising to have DEA replicate its dragnet using SPCMA. There's no sign, yet, that DEA has been included under FAA certifications (and there's not, as far as we know, an FAA narcotics certificate). But EO 12333 sharing with DEA would be easier to implement on the sly than FAA sharing. And once you've shared with DEA, you might as well share with everyone else.

Finally, this imminent change is why I was so insistent that SPCMA should have been in the Brennan Center's report on privacy implications of EO 12333 collection. What the government was doing, explicitly, in 2007 when they rolled that out was making the US person participants in internationally collected data visible. We've seen inklings of how NSA coaches analysts to target foreigners to get at that US person content. The implications of basing targeting off of SPCMA enabled analysis under PRISM (which we know they do because DOJ turned over the SPCMA document, but not the backup, to FISC during the Yahoo challenge), currently, are that US person data can get selected *because US persons are involved* and then handed over to FBI with no limits on its access. Doing so under EO 12333 will only expand the amount of data available — and because of the structure of the Internet, a great deal of it is available.

Probably, the best way to combat this change is to vastly expand the language of FAA 703-705 to over US person data collected incidentally overseas during next year's FAA reauthorization. But it will take language like that, because simply pointing to FISA will not change the Executive's ability to change EO 12333 — even secretly! — at will.

THE BLIND SPOTS BRENNAN CENTER'S EO 12333 REPORT

The Brennan Center released a report on EO 12333 Thursday that aims to spark a debate about the privacy impacts of (just) NSA's surveillance overseas, in part by describing the privacy impacts of EO 12333.

> In contrast, there has been relatively little public or congressional debate within the United States about the NSA's overseas surveillance operations, which are governed primarily by Executive Order (EO) 12333—a presidential directive issued by Ronald Reagan in 1981 and revised by subsequent administrations. These activities, which involve the collection of communications content and metadata alike, constitute the majority of the NSA's surveillance operations, yet they have largely escaped public scrutiny.
>
> There are several reasons why EO 12333 and the programs that operate under its aegis have gone largely unnoticed. One is the misconception that overseas surveillance presents little privacy risk to Americans. Another is the scant information in the public domain about how EO 12333 actually operates. Finally, the few regulations that are public create a confusing and sometimes internally inconsistent thicket of guidelines.

Unfortunately the report misses some of the biggest threats EO 12333 surveillance poses to Americans' privacy. Indeed, the report reads

more like a hodgepodge of some risks, rather than a report on the ways in which the NSA and other agencies can spy on Americans overseas. When attempting to define the political battlefield in which future fights for reform will happen, we can't afford to miss any ground.

Historical and technical discussion

Brennan's excellent report on the FISA Court (like this report, written by Liza Goitein and Faiza Patel, though Amos Toh also worked on this recent report) started with a history of how we got to where we are now, with the FISA Court approving entire surveillance programs in secret. This report would have profited from doing the same. It would have contextualized EO 12333, as the third of a series of EOs issued in the wake of the *Keith* decision and the Church Committee, which arose out of a separation of powers debate between the Executive and Congress. It could have described the few details we know of the largely unknown process by which EO 12333's protections for Americans started breaking down. It would have described how, with Stellar Wind, the Executive blew off FISA and secretly rewrote EO 12333 without notice to spy on Americans (in part by turning an existing DEA dragnet, which was at least partly authorized by domestic statute, inward). It would have described how, in the wake of the hospital confrontation, the Executive moved most of those activities under FISA, only to start moving them back (most notably with Internet metadata) as FISA again proved too restrictive, even as technology made bypassing FISA easier.

The discussion also would benefit from more discussion of the telecommunications infrastructure of the world, how packets get routed across it, and how tech companies (and the NSA!) operate servers in multiple places around the globe. As an example, the report

discusses XKeyscore as a “database” even while linking to an article that describes it as a “a fully distributed processing and query system that runs on machines around the world.” I get using “database” as shorthand for repositories — I’ve done it myself, particularly for the federated queries that chained metadata from both Section 215, PRTT, and 12333 collection in unified queries (and in so doing alerted analysts when the same queries could be run entirely under EO 12333 and so be covered by more flexible rules). But understanding how that collect-and-query process exploits the flows of data across the Internet is key to understanding how even Americans talking to Americans can be exposed — but also to giving the NSA’s protections for US persons a fair shake (one of NSA’s most common Intelligence Oversight Board violations, from what we can see of the often redacted reports, seem to be about query construction, which shows NSA polices that part of the process closely). The privacy threat to Americans from EO 12333 authorized SIGINT stems from a “Collect it all” mentality and the structure of the Internet— not from any discreet programs that employ a different approach for one particular country or unencrypted data source.

Treatment of SPCMA

I’m most baffled by the report’s silence on Special Procedures for Communications Metadata Analysis, SPCMA, especially given the report’s extended (and worthwhile) discussion of the word games DOD plays with “collection” and other terms, as in this passage based on language in place up until the moment DOJ started implementing SPCMA in 2007.

> The Intelligence Law Handbook indicates that for intelligence agencies housed under the DoD, the act of “collection” is “more than ‘gathering’ — it could be described as ‘gathering, plus…’”91 But what additional action is required to

> complete “collection” depends on which agency you ask and which document you rely on. This makes it difficult to determine which rules, if any, apply when an intelligence agency gathers information. Our analysis shows that there are at least three definitions of “collection”:
>
> 1) the process by which information obtained is rendered “intelligible” to human understanding;
>
> 2) the process by which analysts filter out information they want from the information obtained; and
>
> 3) the gathering or obtaining of information (i.e., the ordinary meaning of the word “collection”).
>
> Since EO 12333 procedures are triggered only upon “collection,” this ambiguity potentially allows the NSA to avoid restrictions simply by categorizing certain information as not having been “collected.”

After all, SPCMA involved precisely those same kinds of word games, creating a virgin birth for data collected overseas.

> 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.”

And those procedures were adopted explicitly in the service of being able to include US person data in EO 12333 analysis.

> The Supplemental Procedures, attached at Tab A, would clarify that the National Security Agency (NSA) may analyze communications metadata associated with United States persons and persons believed to be in the United States.

In 2007, the government made an affirmative effort to be able to integrate foreign collected US person metadata into NSA's analysis. It did so at a time when it was also working toward greater information-sharing between agencies (under ICREACH) and at a time when first getting the FISA Court to sanction the use of contact chaining — integrating SPCMA, though without revealing the rationale behind SPCMA!!! — as a basis for conducting domestic collection under Protect America Act. Starting in 2009 and significantly by 2011, the NSA replaced a huge domestic dragnet (one limited to counterterrorism purposes and with strict sharing rules), in part, with SPCMA (which has neither the counterterrorism limit nor the strict dissemination rules).

~~(TS//SI//NF)~~ **Other authorities can satisfy certain foreign intelligence requirements that the PR/TT program was designed to meet.** The Supplemental Procedures Governing Communications Metadata Analysis (SPCMA), which SID implemented widely in late 2010, allows NSA to call-chain from, to, or through U.S. person selectors in Signals Intelligence collection obtained under a number of authorities. In addition, notwithstanding restrictions stemming from the FISC's recent concerns regarding upstream collection, FAA §702 has emerged as another critical source for collection of Internet communications of foreign terrorists. Thus, SPCMA and FAA §702 assist in the identification of terrorists communicating with individuals within the United States, which addresses one of the original reasons for establishing the PR/TT program in 2004.

In other words, amid all the examples the Brennan Report gives for how Americans might be surveilled by NSA under EO 12333 (which underplay the exposure both for international calls placed from the US and entirely domestic Internet communication), it doesn't mention the one that had analysis including US person metadata as the explicit purpose.

Or to put it more simply, in 2007, at a time when the structure of international communication was such that it was possible to spy on entirely domestic communications

overseas, the government either adopted or (my suspicion) resumed analyzing US person metadata collected overseas. That seems worth mentioning in a report on how Americans can be exposed under EO 12333. (I asked Patel why SPCMA was not included in the report but have gotten no response.) In terms of the political fight, that's the difference between a politician trying to fight for more US person protections being called "speculative" and that same politician being able to point to actual evidence EO 12333 collection has implicated Americans' privacy.

Other agencies

Finally, any discussion of the surveillance exposure of Americans under EO 12333 should, in my opinion, scope more broadly to include other agencies. I would include CIA (not least because PCLOB identified two CIA programs that appear to affect US persons) and Treasury (which tracks a great deal of international financial flows, even of Americans with ties to sanctioned countries; the report as a whole is unduly focused just on communications data).

But I would start with a discussion of (or at least questions we need answered about) DEA. After all, international drug investigations have always been included in EO 12333's US person collection permissions.

> Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order, after consultation with the Director. Those procedures shall permit collection, retention, and dissemination of the following types of information:

> (c) Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation;

DEA engages in a great deal of information collection on its own right (and shares with with FBI, though the FBI went to some length to hide details of such sharing from DOJ's Inspector General). We know many of the technologies first used on our foreign adversaries sometimes get introduced for use with Americans via DEA, most notably with that massive metadata dragnet. And DEA doesn't have the same strict definition as a foreign intelligence organization as NSA, making the potential impact of overseas collection more direct for Americans. Plus, as the Brennan Report notes, DEA (along with Treasury) has never been in compliance with EO 12333's requirement for enacting procedures.

I get that when non-experts think of surveillance they think of NSA. But that's a problem, not just because NSA currently more closely hews to the rules such as they are given than DEA, CIA, and FBI are believed to do, but also because NSA has never posed the biggest threat to Americans as agencies that have the ability to prosecute Americans like FBI and DEA. If you're going to write a report framing the debate, shouldn't it frame it in a way that ties directly to the impact of it, even if we know far less about those areas that may have more direct impact?

This report feels like one written in the belief that you best understand surveillance by talking about law largely in isolation from technology and bureaucracy. That's always problematic — indeed, the report suffers from some of the same blind spots that the debate about USA Freedom Act did, based as it was in knowledge about the Section 215 statute but little knowledge of its statutorily mandated minimization procedures. It's especially

problematic when writing about programs that operate in the space not limited by any law, where executive power is at its zenith.

Absent further successful effort to expand Congress' authority over surveillance (the report describes Section 309 of last year's Intelligence Authorization but doesn't focus on Sections 703 through 705 of FISA Amendments Act, an earlier attempt to carve out protections for Americans under EO 12333), technology, not the law, sets the biggest limits on what the Executive can do under EO 12333.

It is time to focus more attention on EO 12333 and I'm grateful the Brennan Report has focused attention on EO 12333. But that focus should include all the ways, including the most central ones, it affects Americans.

ALBERTO GONZALES REJECTED DHS' EO 12333 PROCEDURES IN 2006

I'm lost down a rabbit hole of declarations relating to ACLU's FOIA on EO 12333 documents (through which John Yoo's Stellar Wind justification for Colleen Kollar-Kotelly was released). Arthur Sepeta, DHS' declarant, had to explain the withholding of just one document, something that shows up on DOJ National Security Division's Vaughn Index.

Sepeta's explanation reveals that in 2006, DHS Secretary Michael Chertoff submitted some guidelines on the collection, retention, and dissemination of US person person information to comply with EO 12333. But Attorney General Alberto Gonzales rejected those guidelines. And, as Sepeta makes clear, DHS *still* doesn't have

any guidelines.

> In this case, NSD 2 is a draft of the DHS Procedures Governing Activities of the Office oflntelligence and Analysis that Affect United States Persons. Section 2.3 of Executive Order No. 12,333 requires the head of an Intelligence Community element or the head of a Department containing an Intelligence Community element to issue "procedures" concerning the collection, retention, and dissemination of information concerning United States persons, after the Attorney General approves the procedures. On April 3, 2006, as required by section 2.3 of Executive Order No. 12,333, the Secretary of Homeland Security, as the head of a Department containing an Intelligence Community element, submitted draft Procedures Governing Activities of the Office of Intelligence and Analysis that Affect United States Persons for approval by the Attorney General. The Attorney General subsequently declined to approve the draft procedures submitted by the Secretary of Homeland Security and inter-agency negotiations over the content of these procedures remain ongoing to this day.

As I noted a year ago, in 2008, DHS adopted interim procedures, but they still haven't finalized any.

Mind you, given the people involved, it's unclear whether Gonzales' rejection of DHS' initial attempt is a good sign or bad sign.

Still, you'd think after 10 years, they would have adopted something?

THAT TIME WHEN JOHN YOO DEEMED EO 12333 OPTIONAL (WORKING THREAD)

I Con the Record has just released the May 17, 2002 letter John Yoo wrote to Colleen Kollar-Kotelly justifying Stellar Wind. This either lays out for the first time or repeats Yoo's claim — which I first reported in 2007, based on a Sheldon Whitehouse Senate address, here — that the President doesn't have to follow EO 12333.

This will be a working thread.

(2) Note Yoo says the attacks caused 5,000 deaths, well beyond the time when authorities knew it to be closer to 3,000.

(2) Yoo mentioned the anthrax attack. Did NSA use Stellar Wind to investigate it?

(2) Yoo uses a more moderate justification here — military being deployed to protect buildings — than Goldsmith did in his 2004 memo, where he talked about specific military flights.

(2) Check EO on creating Homeland Security office on domestic program.

(2) As soon as Yoo starts talking about Stellar Wind, he adopts the conditional tense: "Electronic surveillance techniques would be part of this effort." This of course follows on Yoo admitting Congress modified FISA (though he doesn't name the statute).

(2) Note in this really squirrelly hypothetical section, Yoo says the surveillance could include email "within" the US, which would be entirely domestic.

(2-3) Note throughout Yoo describes Bush as

"Chief Executive."

(3) Yoo points to absence of a charter as basis for doing whatever NSA wants.

(3) "Congress, however, has not imposed any express statutory restrictions on the NSA's ability to intercept communications that involve United States citizens or that occur domestically." (based on the absence of such language in NSA)

(4) I believe the second redaction is designed to enable the wiretapping of people claimed to be tied to the anthrax attack.

(5) Here's the passage that said EO 12333 is optional.

Even if surveillance were to conflicts with Executive Order 12,333, it could not be said to be illegal. An executive order is only the expression of the President's exercise of his inherent constitutional powers. Thus, an executive order cannot limit a President, just as one President cannot legally bind future Presidents in areas of the executive's Article II authority. Further, there is no constitutional requirement that a President issue a new executive order whenever he wishes to depart from the terms of a previous executive order. In exercising his constitutional or delegated statutory powers, the President often must issue instructions to his subordinates in the executive branch, which takes the form of an executive order. An executive order, in no sense then, represents a command from the President to himself, and therefore an executive order does not commit the President himself to a certain course of action. Rather than "violate" an executive order, the President in authorizing a departure from an executive order has instead modified or waived it. Memorandum for the Attorney General, From: Charles J. Cooper, Assistant Attorney General, *Re: Legal Authority for Recent Covert Arms Transfers to Iran* (Dec. 17, 1986). In doing so,

(4-5) I find Yoo's language the more troubling given what precedes it — the rationale.

the United States. The only qualification on domestic collection is that it cannot be undertaken to acquire information about the domestic activities of United States persons. If United States persons were engaged in terrorist activities, either by communicating with members of Al Qaeda [redacted] or by communicating with foreign terrorists even within the United States, they are not engaging in purely "domestic" activities. Instead, they are participating in foreign terrorist activities that have a component within the United States. We do not believe that Executive Order 12,333 was intended to prohibit intelligence agencies from tracking international terrorist activities, solely because terrorists conduct those activities within the United States. This would create the odd incentive of providing international terrorists with more freedom to conduct their illegal activities *inside* the United States than outside of it. Rather, the Executive Order was meant to protect the privacy of United States persons where foreign threats were not involved. Further, Section 2.4 of Executive Order 12,333 contemplates that the NSA and other

I'll come back to this, but note how "domestic" gets defined here. Much of this is still on the books and explains why Muslims get treated differently.

(5, 6) Note Yoo's explanation for doing this off the books.

1. Need for secrecy
2. Inability to get FISC to approve bulk content collection or domestic

metadata collection
3. No knowledge of identity of target

That’s not speed, which later became the excuse

(5) “FISA only provides a safe harbor for electronic surveillance, and cannot restrict the President’s ability to engage in warrantless searches that protect the national security.”

(5) Note Yoo refers to the metadata dragnet as “general collection,” which sounds an awful lot like a general warrant.

(7) The redactions on 7 are especially interesting given likelihood they conflict with either what K-K, Bates, or Howard subsequently approved.

(8) The timing of this is remarkable. This letter was written on the same date that Ashcroft changed the rules on the wall, which Lamberth unsuccessfully tried to impose some limits on. Then, on July 22, OLC further expanded the GJ sharing address in FN 8.

(8) Note, again, how Yoo is rewriting Keith and Katz.

(10) again, Yoo seems to be laying the groundwork for back door searches, which makes me wonder whether that’s why this got released?

(12) I don’t believe this border exception appears in Goldsmith. Which suggests there’s something with the way this was applied that is particularly problematic.

(13) This must be the language in question. Goldsmith used another means to justify cross-border collection, while admitting it outright.

(14) This language also disappears from later justifications, suggesting it is part of the problem.

properly route the communication. A reasonable person could be expected to know that an ISP would record such message information for their own business purposes, just as telephone companies record phone numbers dialed. Furthermore, other information such as routing and server information is not even part of the content of a message written by the sender. Rather, such information is generated by the ISP itself, as part of its routine business operations, to help it send the electronic message through its network to the correct recipient. A sender could have no legitimate expectation of privacy over information he did not even include in his message, but instead is created by the ISP as part of its own business processes. A person would have no more privacy interest in that information than he would have in a postmark stamped onto the outside of an envelope containing his letter.

The discussion continues onto the next page. It is of particular interest that K-K got this letter, given that her category distinctions probably addressed these distinctions.

(15) Bingo. This might be a very simple explanation for why they had to go to FISC.

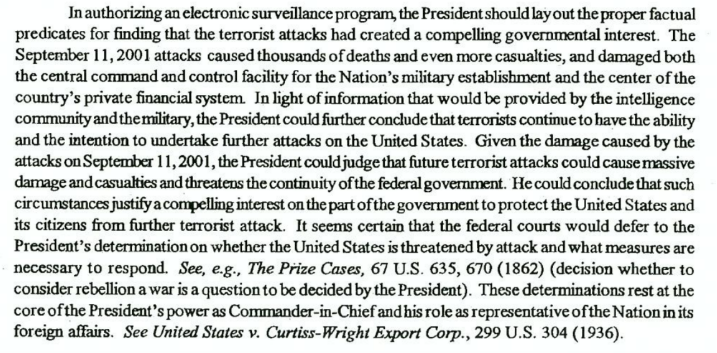
Congress extended pen register authority to surveillance of electronic mail, it also subjected that authority to the general restrictions of Title III and FISA, which require the Justice Department to obtain an ex parte court order before using such devices. While the requirements for such an order are minimal, see 18 U.S.C. § 3122 (government attorney must certify only that information likely to be gained from pen register "is relevant to an ongoing criminal investigation being conducted by that agency"), a warrantless surveillance program would not seek a judicial order for the surveillance program here. Title III attempts to forbid the use of pen registers or, now, electronic mail trap and trace devices, without a court under Title III or FISA.

(17) This passage about picking the Defense Secretary rather than AG is pretty much what I noted in my post on the underyling 4A argument, but it has ramifications for the post-2004 program. Also note how closely it piggybacks with the changes to AG guidelines and the

Thus, the Fourth Amendment should not limit military operations to prevent attacks that take place within the American homeland, just as it would not limit the President's power to respond to attacks launched abroad. A surveillance program, undertaken for national security purposes, would be a necessary element in the effective exercise of the President's authority to prosecute the current war successfully. Intelligence gathered through surveillance allows the Commander-in-Chief to determine how best to position and deploy the Armed Forces. It seems clear that the primary purpose of the surveillance program is to defend the national security, rather than for law enforcement purposes, which might trigger Fourth Amendment concerns. In this respect, it is significant that the President would be ordering the Secretary of Defense (who supervises the NSA), rather than the Justice Department, to conduct the surveillance, and that evidence would not be preserved for later use in criminal investigations. While such secondary use of such information for law enforcement does not undermine the primary national security purpose motivating the surveillance program, it is also clear that such intelligence material, once developed, can be made available to the Justice Department for domestic use.

This language explains why they weren't looking in Stellar Wind for Brady material, and also explains how they do parallel construction (which plays out in the IG Report).

(19) This section lays out the need for the scary memos, without revealing to K-K they exist.



In authorizing an electronic surveillance program, the President should lay out the proper factual predicates for finding that the terrorist attacks had created a compelling governmental interest. The September 11, 2001 attacks caused thousands of deaths and even more casualties, and damaged both the central command and control facility for the Nation's military establishment and the center of the country's private financial system. In light of information that would be provided by the intelligence community and the military, the President could further conclude that terrorists continue to have the ability and the intention to undertake further attacks on the United States. Given the damage caused by the attacks on September 11, 2001, the President could judge that future terrorist attacks could cause massive damage and casualties and threatens the continuity of the federal government. He could conclude that such circumstances justify a compelling interest on the part of the government to protect the United States and its citizens from further terrorist attack. It seems certain that the federal courts would defer to the President's determination on whether the United States is threatened by attack and what measures are necessary to respond. *See, e.g., The Prize Cases,* 67 U.S. 635, 670 (1862) (decision whether to consider rebellion a war is a question to be decided by the President). These determinations rest at the core of the President's power as Commander-in-Chief and his role as representative of the Nation in its foreign affairs. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304 (1936).

(21) The big redacted section—the biggest redaction in the letter—suggests they're still hiding the capture and pull up method of this, and therefore the sheer bulk of all this. That's all the more interesting given that the wall was coming down at that moment. The other redactions in this section, too, seem to track the indexing function. Again, it's interesting K-K had read (or reviewed) this before the PRTT discussion.

PCLOB'S NEW WORK: EXAMINING "ACTIVITIES" TAKING PLACE IN THE LOOPHOLES OF EO 12333

On Wednesday, the Privacy and Civil Liberties Oversight Board met to approve its next project. They are just about completing a general overview of the Intelligence Community's use of EO 12333 (as part of which they've been nagging

agencies, notably DEA and Treasury, to comply with requirements imposed by Ronald Reagan). Next, they will move onto a deep dive of two programs conducted under EO 12333, one each for NSA and CIA. PCLOB has now posted materials from Wednesday's meeting, though this overview is also useful.

Keeping in mind that PCLOB already has a pretty good sense of what the agencies are doing, consider this description of its deep dive into activities of NSA and CIA.

> During the next stage of its inquiry, the Board will select two counterterrorism-related activities governed by E.O. 12333, and will then conduct focused, in-depth examinations of those activities. The Board plans to concentrate on activities of the CIA and NSA, and to select activities that involve one or more of the following: (1) bulk collection involving a significant chance of acquiring U.S. person information; (2) use of incidentally collected U.S. person information; (3) targeting of U.S. persons; and (4) collection that occurs within the United States or from U.S. companies. Both reviews will involve assessing how the need for the activity in question is balanced with the need to protect privacy and civil liberties. The reviews will result in written reports and, if appropriate, recommendations for the enhancement of civil liberties and privacy.

Some of this is unsurprising. If PCLOB were to conduct a review of SPCMA, it would be assessing NSA's analysis of incidentally collected US person data collected in great volume as a result of collecting in bulk. Indeed, conducting such a review would get to a lot of the issues raised by John Napier Tye in PCLOB testimony.

But I'm more interested in bullets 3 and 4.

Bullet 3 suggests that CIA and/or NSA are targeting US persons under EO 12333.

There are certainly ways that's permissible. For example, EO 12333 permits agencies to conduct physical surveillance of their employees.

> (1) Physical surveillance of present or former employees, present or former intelligence element contractors or their present or former employees, or applicants for any such employment or contracting; and
>
> (2) Physical surveillance of a military person employed by a non-intelligence element of a military service;

And it permits physical surveillance overseas if significant information can't reasonably acquired by other means.

> Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means.

You'd think this would bump up against the FISA Amendments Act very quickly, but remember that this EO was updated in the days after FAA was completed, so everything in it likely accounts for FAA.

On that note, this useful post from Jonathan Mayer (click through for the handy graphic) describes how NSA's classified EO 12333 permits the Attorney General to authorize the surveillance of US persons or entities for limited periods of time.

> A third area of Executive Order 12333, on American soil, is the "Classified Annex Authority" or "CAA." Its source is a classified addition to Executive Order 12333, set out in an NSA policy document.[13] The most recent revision,

> from 2009, reads:
>
> > Communications of or concerning a United States person[14] may be intercepted intentionally or selected deliberately . . .
> >
> > 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.
>
> That provision appears to allow the Attorney General to unilaterally trump FISA. I'm not*entirely* confident that's what it means, but it sure looks like it.[15]
>
> I'm skeptical that the executive branch can just brush aside FISA, especially on American soil. In Justice Jackson's famous phrasing, when the executive branch acts in clear violation of a legislative enactment, its "power is at its lowest ebb." Nevertheless, the executive branch does appear to claim that Article II can override FISA, and it does appear to have invoked this Classified Annex Authority on occasion.[16]

Finally, remember that CIA has conducted investigations targeting Senate Intelligence Committee staffers, which suggests it interprets its ability to conduct counterintelligence investigations unbelievably broadly.

Then there's bullet 4, which suggests CIA and/or NSA are collecting "within the United States or from U.S. companies."

With regards collection "within the US," Mayer's post is helpful here too, pointing to loopholes for wireless and satellite communication.

> The law that results is quite counterintuitive. If a communication is carried by radio waves, and it's one-end foreign, it falls under Executive Order 12333. If that same communication were carried by a wire, though, it would fall under FISA. (Specifically, the Section 702 upstream program.)
>
> As for how this Executive Order 12333 authority might be used beyond satellite surveillance, I could only speculate. Perhaps intercepting cellphone calls to or from foreign embassies?[12] Or along the national borders? At any rate, the FISA-free domestic wireless authority appears to be even broader than the Transit Authority.

As far as collection outside the US, this may simply be a reference to providers voluntarily providing data under 18 U.S.C. § 2511(2)(f), as we know at least some of the telecoms do.

But we also know NSA and its partner GCHQ have stolen unencrypted US company data overseas. And while the theft off Google's fiber has, hopefully, been stopped, there's still quite a lot of ways NSA can steal this data.

In any case, the terms of PCLOB's investigation sure seem to suggest that CIA and/or NSA are exploiting the holes in EO 12333 in significant enough ways to raise concerns for PCLOB.

GOVERNMENT'S ASSASSINATION OF ANWAR AL-AWLAKI USED "SIGNIFICANTLY DIFFERENT" EO 12333 ANALYSIS

Jameel Jaffer has a post on the government's latest crazy-talk in the ongoing ACLU and NYT effort to liberate more drone memos. He describes how — in the government's response to their appeal of the latest decisions on the Anwar al-Awlaki FOIA — the government claims the Court's release of an OLC memo does not constitute official release of that memo. (Note, I wouldn't be surprised if the government is making this claim in anticipation of orders to release torture pictures in ACLU's torture FOIA suit that's about to head to the 2nd Circuit.)

But there's another interesting aspect of that brief. It provides heavily redacted discussion of the things Judge Colleen McMahon permitted the government to withhold. But it makes it clear that one of those things is a March 2002 OLC memo that offers different analysis about the assassination ban than the analysis used to kill Anwar al-Awlaki.

> The district court also upheld the withholding of a March 2002 OLC Memorandum analyzing the assassination ban in Executive Order 12,333 (the "March 2002 Memorandum"). (CA 468-70; see CA 315-29). Although the district court noted that the OLC-DOD Memorandum released by this Court contained a "brief mention" of Executive Order 12,333, the district court concluded that the analysis in the March 2002 Memorandum is significantly different

> from any legal analysis that this Court held has been officially disclosed and for which privilege has been waived.

The statement here is carefully worded, probably for good reason. That's because the February 19, 2010 memo McMahon permitted the government to almost entirely redact clearly explains EO 123333 and its purported ban on assassinations in more depth than the July 16, 2010 one; the first paragraph ends,

> Under the conditions and factual predicates as represented by the CIA and in the materials provided to us from the Intelligence Community, we believed that a decisionmaker, on the basis of such information, could reasonably conclude that the use of lethal force against Aulaqi would not violate the assassination ban in Executive Order 12333 or any application constitutional limitations due to Aulaqi's United States citizenship.

I pointed out that there must be more assassination analysis here. It almost certainly resembles what Harold Koh said about a month later, for which activists at NYU are now calling into question his suitability as an international law professor.

> Fourth and finally, some have argued that our targeting practices violate *domestic law,* in particular, the long-standing *domestic ban on assassinations*. But under domestic law, the use of lawful weapons systems—consistent with the applicable laws of war—for precision targeting of specific high-level belligerent leaders when acting in self-defense or during an armed conflict is not unlawful, and hence does not constitute "assassination."

But the government is claiming that because that

didn’t get disclosed in the July 2010 memo, it doesn’t have to be disclosed in the February 2010 memo, and the earlier “significantly different” analysis from OLC doesn’t have to be disclosed either.

At a minimum, ACLU and NYT ought to be able to point to the language in the white paper that addresses assassinations that doesn’t appear in the later memo to show that the government has already disclosed it.

But I’m just as interested that OLC had to change its previous stance on assassinations to be able to kill Awlaki.

Of course, the earlier memo was written during a period when John Yoo and others were pixie dusting EO 12333, basically saying the President didn’t have to abide by EO 12333, but could instead violate it and call that modifying it. Perhaps that’s the difference — that David Barron invented a way to say that killing a high ranking leader (whether or not he’s a citizen) didn’t constitute assassination because of the weapons systems involved, as distinct from saying the President could blow off his own EOs in secret and not tell anyone.

I suggested Dick Cheney had likely pixie dusted EO 12333’s ban on assassinations back in 2009.

But there’s also the possibility the government had to reverse the earlier decision in some other fashion. After all, when Kamal Derwish was killed in a drone strike in Yemen on November 9, 2002, the government claimed Abu Ali al-Harithi was the target, a claim the government made about its December 24, 2009 attempt to kill Anwar al-Awlaki, but one they dropped in all subsequent attempts, coincident with the February 2010 memo. That is, while I think it less likely than the alternative, it is possible that the 2010 analysis is “significantly different” because they had to interpret the assassination ban even more permissively. While I do think it less likely, it might explain why Senators Wyden, Udall, and Heinrich keep pushing

for more disclosure on this issue.

One thing is clear, however. The fact that the government can conduct “significantly different” analysis of what EO 12333 means, in secret, anytime it wants to wiretap or kill a US citizen makes clear that it is not a meaningful limit on Executive power.