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.