WORKING THREAD: NEW AND IMPROVED DRAGNETTERY

I Con the Record has released a series of changes to the dragnet to fulfill President Obama's directive to improve privacy. This will be a working thread.

Seeking Independent Advice

This section lays out all the independent advice the IC has sought in the last 18 months, from the advice largely ignored (President's Review Group) to narrowly scoped (the National Academies of Science report that assessed whether the IC could get the same features of the current phone dragnet, without assessing whether it was effective) to the largely inane (Congressional hearings).

It doesn't really address whether it's using this advice effectively. There seems to be an underlying efficacy question still missing.

Privacy and Civil Liberties Protections

This appears to be the meat of the report.

It starts by linking to the interim report that basically exempted the most privacy intrusive parts of NSA's dragnet — bulk collection and research — from its privacy protections.

It then links all the agencies' efforts to implement

- **Office of the Director of National Intelligence**
- **Central Intelligence Agency**
- **National Security Agency**
- **National Reconnaissance Office**
- **Federal Bureau of Investigation**

- **Department of Homeland Security**
- **Drug Enforcement Agency**
- **State Department**
- **Treasury Department**
- **Department of Energy**
- **U.S. Coast Guard**
- Other IC Elements in the Department of Defense

These will take closer review. Note that DEA's report only covers its Office of National Security Intelligence, which seems to suggest there's a lot more — a whole lot more — intelligence that falls outside this area. And it's really perfunctory. Compare the storage section with that of DHS, which at least has standards it has to meet for the security of the data it keeps (even if we know DHS is so technologically backwards they can't really meet this).

FBI

I can already see some problems with FBI's entry (which conveniently cannot be cut and paste). For example, it assumes any minimized data it receives adheres to certain standards. "Unless it possesses specific information to the contrary, the FBI will presume that any evaluated or minimized section 702 information it receives from other IC elements meets these standards." The recently liberated 702 report showed that this left a bit of gap in compliance.

Then there's the exception that eats the rule, in which prohibits FBI from keeping any unevaluated non-US person data for longer than 5 years "unless retention of comparable information concerning U.S. persons would be permitted under section 2.3 of Executive Order 12333." FBI's interpretation of exceptions here are very broad.

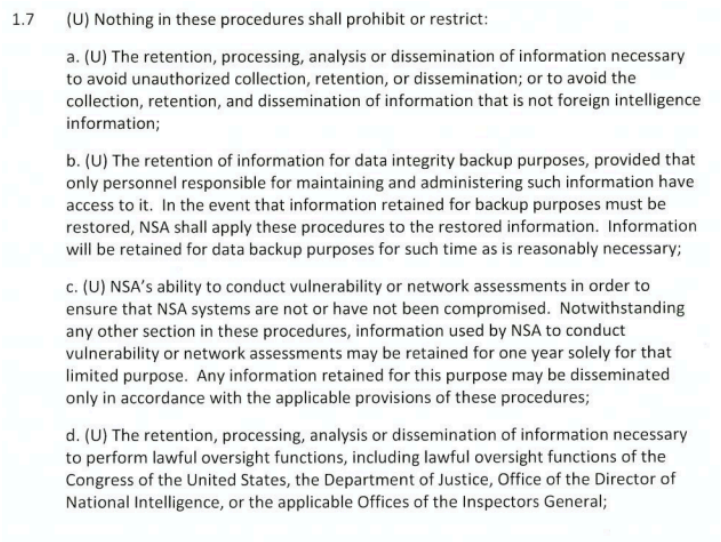
FBI's queries language is not tied to law enforcement investigations. That likely means that it retains the ability to do queries for assessments, which require no evidence of wrong-doing.

When FBI talks about oversight, it describes "periodic auditing." Given that the 702 IG report showed that FBI had basically blown off statutory requirements for auditing and reports for 2 of 3 years reviewed, I'd like to see something more concrete than this…

Incidentally, note that FBI just signed this on February 2. It appears they were the last (or among the last) agencies to finish these (probably after deadline, too, as this was supposed to be rolled out on the 1 year anniversary of Obama's speech).

NSA

There are some interesting exceptions in the NSA report, including the ginormous one for bulk collection. I'm particularly interested in a few of these:



1.7 (U) Nothing in these procedures shall prohibit or restrict:

a. (U) The retention, processing, analysis or dissemination of information necessary to avoid unauthorized collection, retention, or dissemination; or to avoid the collection, retention, and dissemination of information that is not foreign intelligence information;

b. (U) The retention of information for data integrity backup purposes, provided that only personnel responsible for maintaining and administering such information have access to it. In the event that information retained for backup purposes must be restored, NSA shall apply these procedures to the restored information. Information will be retained for data backup purposes for such time as is reasonably necessary;

c. (U) NSA's ability to conduct vulnerability or network assessments in order to ensure that NSA systems are not or have not been compromised. Notwithstanding any other section in these procedures, information used by NSA to conduct vulnerability or network assessments may be retained for one year solely for that limited purpose. Any information retained for this purpose may be disseminated only in accordance with the applicable provisions of these procedures;

d. (U) The retention, processing, analysis or dissemination of information necessary to perform lawful oversight functions, including lawful oversight functions of the Congress of the United States, the Department of Justice, Office of the Director of National Intelligence, or the applicable Offices of the Inspectors General;

The economic advantage language appears to get weaker and weaker in here. It now states that identifying trade violations does not constitute a competitive advantage. It also permits the collection of private trade secrets for national

security purposes — which is what China would say it is doing when it steals our secrets.

I think the retention language has gotten slightly broader, now. The encrypted communication exception has been rewritten to include anything not processed into intelligible form.

It also states, "personal information about the routine activities of a non-U.S. person would not be disseminated without some indication that the personal information is related to an authorized foreign intelligence requirement." Consider how this language would work for what we know to have been spying on the online sex habits of people the US wants to discredit. First, they only need "some indication" that the dissemination is tied to a FI requirement. There's also that word, "related to," which as we know now means "all." In other words, this exception would still permit really intrusive spying, if we thought the target was a nice FI target.

Others

Love this from DOE: "The origins of specific information contained in evaluated or finished intelligence products—or the specific means by which such information was collected—may not in all cases be evident to DOE-IN or DOE as a recipient of such intelligence products." State has a very similar caveat.

Non-NSA DOD components just adopted NSA's document.

Judicial Redress

Any bets we'll give Saudis judicial redress?

> In furtherance of its commitment to protecting privacy in the law enforcement context, the Administration is working with Members of Congress on legislation to give citizens of designated countries the right to seek

> judicial redress for intentional or willful disclosures of protected information, and for refusal to grant access or to rectify any errors in that information.

Section 215

Note the "such as" in this section:

> Section 215 of the USA PATRIOT Act authorizes the Government to make requests to the Foreign Intelligence Surveillance Court (FISC) for orders requiring production of documents or other tangible things (books, records, papers, documents, and other items) when they are relevant to an authorized national security investigation *such as* an investigation to protect against international terrorism or clandestine intelligence activities.

I find it interesting ODNI departed from statutory law (which is about foreign powers) here. I suspect it suggests we're using non-bulk Section 215 more in other "such as" investigations, "such as" cyber.

Note the section has an odd non-denial denial, first asserting that the "vast majority" of orders are for limited production (many of which, nevertheless, FISC has seen fit to impose minimization procedures on). Then it discusses the phone dragnet. But nowhere does it say those two categories encompass all the possibilities (which we should therefore assume they don't). And that's using IC's incredibly narrow definition of "bulk."

The report says there were only 161 "target identifiers" last year under the phone dragnet. That *appears* to be a pretty significant decline (which may, in part, suggest that a lot of NSA's earlier targets weren't ready for FISC scrutiny), from 423. But IConTheRecord's 2013 transparency report is not 100% clear on this.

LOL. ODNI makes this claim:

> The Attorney General and the Director of National Intelligence stated that, based on communications providers' existing data retention practices, the bill would retain the essential operational capabilities of the existing bulk telephone metadata program while eliminating bulk collection by the government under these legal authorities.

Of course, we learned during the confirmation debate that the government had gotten Verizon — one of the key targets of this legislation — to keep its data longer than the 12 to 18 months it currently does. So this claim is sort of bullshit.

Section 702

ODNI is claiming (and PCLOB is endorsing) that it has answered PCLOB's recommendations. Key among these are the 702 treatment.

Here's how the report says agencies are adding more controls to their back door searches.

> First, FBI, CIA, and NSA each are instituting new requirements for using a U.S. person identifier to query information acquired under Section 702. As recommended by the Privacy and Civil Liberties Oversight Board, NSA's minimization procedures will require a written statement of facts showing that a query is reasonably likely to return foreign intelligence information. CIA's minimization procedures will be similarly amended to require a statement of facts for queries of content. In addition, FBI's minimization procedures will be updated to more clearly reflect the FBI's standard for conducting U.S. person queries and to require additional supervisory approval to access query

> results in certain circumstances.

Remember, CIA's big issue is on metadata searches. This appears to leave those uncounted metadata searches uncounted.

And the FBI stuff is similarly weak: it claims the FBI hasn't been following its own standards (alert! alert! alert!), and that it will add additional controls to access queries. That is, it seems to suggest really big weaknesses, rather than a fix to the problem in general, which is that FBI does too many back door searches to count.

Then the new policy imposes new oversight over FI retention decisions.

> Second, the new policy re-affirms requirements that the government must delete communications to, from, or about U.S. persons acquired under Section 702 that have been determined to lack foreign intelligence value. In addition, the policy requires the Department of Justice and the Office of the Director of National Intelligence to conduct oversight over these retention decisions. This change will help ensure that the Intelligence Community preserves only that information that might help advance its national security mission.

If effective, this will amount to the government having to follow the rules it has been violating. But absent publication of the yearly 702 reviews, I don't think DOJ/ODNI oversight is enough: we'd need to be able to actually measure this (especially since both PCLOB and WaPo showed the IC was totally out of bounds on this front).

I noted this on Twitter, but this claimed change raises real concerns about what prior policy was.

> Third, consistent with the recommendation of the Privacy and Civil Liberties Oversight Board, information acquired under Section 702 about a U.S. person will not be introduced as evidence against that person in any criminal proceeding except (1) with the approval of the Attorney General, and (2) in criminal cases with national security implications or certain other serious crimes. This change will ensure that, if the Department of Justice decides to use information acquired under Section 702 about a U.S. person in a criminal case, it will do so only for national security purposes or in prosecuting the most serious crimes.

FBI had already told PCLOB that it was unlikely to have 702 searches show up non NatSec functions. Does this mean that's wrong? That they've been using it to prosecute minor non-NatSec crimes? Also, what good does this limitation do if FBI can still use the minor crime evidence to coerce informants?

NSLs

Interesting changes to NSLs, but I'm unsure about what it means (other than that DOJ thinks they may lose the EFF suit in the 9th).

> In response to the President's new direction, the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of three years after the opening of a fully predicated investigation or the investigation's close.
>
> Continued nondisclosures orders beyond this period are permitted only if a Special Agent in Charge or a Deputy Assistant Director determines that the statutory standards for nondisclosure continue to be satisfied and that the

> case agent has justified, in writing, why continued nondisclosure is appropriate.

First, 3 years is a long time—more reasonable would be 1 year. But I'm also curious precisely what they mean by "predicated investigation"? Full investigation? Preliminary? What if it's an enterprise investigation?

Also, that justification in writing — I assume that's not to an actual judge?

Minimization procedures

ODNI has released the minimization procedures for FBI, CIA, and NSA (but not for NCTC, which at least as of August 2013, also had Section 702 minimization procedures). I'll come back to these, especially the FBI ones.

But in the meantime, here's what FBI's minimization procedures say about conversations with attorneys for people who have not yet been charged with a crime:

3. ~~(S//NF)~~ Privileged communications involving targets and other persons not charged with a crime in the United States.

~~(S//NF)~~ [redacted]

[redacted]

~~(S//NF)~~ [redacted]