3 TECH ISSUES THE NON-TECHNOLOGIST NSA TECHNICAL COMMITTEE NEEDS TO ADDRESS

A number of people are asking why I'm so shocked that President Obama appointed no technologists for his NSA Review Committee.

Here are three issues that should be central to the Committee's discussions that are, in significant part, technology questions. There are more. But for each of these questions, the discussion should not be whether the Intelligence Community thinks the current solution is the best or only one, but whether it is an appropriate choice given privacy implications and other concerns.

- Whether the Intelligence Community can accomplish the goals of the Section 215 dragnet without collecting all US person metadata
- Whether the NSA can avoid collecting Multiple Communication Transactions as part of upstream collection
- How to oversee unaudited actions of technical personnel

There are just three really obvious issues that should be reviewed by the committee. And for all of them, it would be really useful for someone with the technical background to challenge NSA's claims to be on the committee.

Whether the Intelligence Community can accomplish the goals of the Section 215 dragnet without collecting all US person metadata

One of the most contentious NSA practices — at least as far as most Americans go — is the collection of all US person phone metadata for the Section 215 dragnet. Yet even Keith Alexander has admitted — here in an exchange with Adam Schiff in a House Intelligence Committee hearing on June 18 — that it would be feasible to do it via other means, though perhaps not as easy.

> REP. SCHIFF: General Alexander, I want to ask you — I raised this in closed session, but I'd like to raise it publicly as well — what are the prospects for changing the program such that, rather than the government acquiring the vast amounts of metadata, the telecommunications companies retain the metadata, and then only on those 300 or so occasions where it needs to be queried, you're querying the telecommunications providers for whether they have those business records related to a reasonable, articulable suspicion of a foreign terrorist connection?
>
> GEN. ALEXANDER: I think, jointly, the **FBI and NSA are looking at the architectural framework of how we actually do this program, and what are the advantages and disadvantages of doing each one**. Each case, as you know from our discussions, if you leave it at the service providers, you have a separate set of issues in terms of how you actually get the information, then how you have to go back and get that information, how you follow it down, and the legal authority for them to compel them to keep these records for a certain period of time. **So what we're doing is we're going to look at that, come back to the director of national**

> **intelligence, the administration, and
> then to you all, and give you
> recommendations on that for both the
> House and the Senate**. I do think that
> that's something that we've agreed to
> look at and that we'll do. It's just
> going to take some time. We want to do
> it right. And I think, just to set
> expectations, the concern is speed in
> crisis. How do we do this? And so that's
> what we need to bring back to you, and
> then, I think, have this discussion here
> and let people know where we are on it.
> Anything that you want to add?
>
> REP. SCHIFF: I would — because I would
> strongly encourage us to vigorously
> investigate that potential
> restructuring. Even though there may be
> attendant inefficiencies with it, I
> think that the American people may be
> much more comfortable with the
> telecommunications companies retaining
> those business records, that metadata,
> than the government acquiring it, even
> though the government doesn't query it
> except on very rare occasions.
>
> GEN. ALEXANDER: So it may be something
> like that we bring back and look at. So
> we are going to look at that. And we
> have already committed to doing that,
> and we will do that and go through all
> the details of that. [my emphasis]

Some of the technical issues raised about this
in other venues pertains to the different ways
the telecoms store their data. In particular,
how they collect VOIP data must be a particular
challenge.

The IC has already lied about two issues related
to this issue: First, about the history of legal
regulations on data retention. And about what
they really mean by "speed." Thus, even if they
weren't already predisposed to pick the easiest
solution — or the one that might have benefits

down the line if a President decided to use it
for domestic "terrorists" — it would be useful
to have a technologist on the committee to
challenge NSA's claims about timeliness or data
compatibility.

For those reasons, this makes the 215 dragnet
solution the perfect issue for the NSA review
committee to review. The technical issues here
might be simple enough for Richard Clarke to
address (and he has express concerns about the
dragnet). But in any eventual challenge to NSA's
claims, it'd be really useful to have experts on
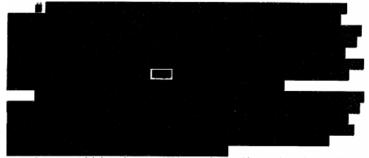data mining making the argument.

**Whether the NSA can avoid collecting MCTs as
part of upstream collection**

When John Bates declared part of the NSA program
unconstitutional on October 3, 2011, a key issue
pertained to whether or not the government could
avoid collecting entirely domestic
communications — whether Single Communication
Transactions or Multiple Communication
Transactions — as part of its upstream
collection.

Bates appeared particularly skeptical about the
government's claims about MCTs.

See Sept. 7, 2011 Hearing Tr. at 69-70, 74. For purposes of this discussion, the Court further
accepts the government's assertion that it is not feasible for NSA to avoid the collection of MCTs
as part of its upstream collection or to limit its collection only to the specific portion or portions
of each transaction that contains the targeted selector. See id. at 48-50; June 1 Submission at
27.[54] The Court therefore concludes that NSA's minimization procedures are, given the current

In his discussion (see page 58), he assumes "for
purposes of this discussion" that government
assertions about the technical challenge are
true. But then he includes a long footnote
modifying that assumption, which has been
entirely redacted save his exhortation that "it
is incumbent upon NSA to continue working to
enhance its capabilities to limit acquisitions
only to targeted communications."

In any event, it is incumbent upon NSA to continue working to enhance its capability to limit acquisitions only to targeted communications.

I don't think Bates entirely buys the government's assertions. Technical folks here and elsewhere have also challenged the claim that the government can't break up MCTs and destroy the US person content.

Moreover, this is an issue that goes to the core of the government's deceit on this issue: given that prior minimization procedures made special exception in data retention guidelines for this collection, it is not credible that the government only came to understand the problem with the collection in May 2011, when they alerted FISC. Given that misrepresentation, it behooves the committee to assess NSA's claims on this issue skeptically.

Finally, this is perhaps the most important issue going forward, given that many in the national security establishment — including Richard Clarke — envision using this technique (though sorting for malicious code rather than foreign intelligence selectors) to combat cyberattacks. The NSA has clear incentives — to accomplish its domestic cybersecurity mission, not its foreign intelligence collection mission — to pretend it can't help itself here. It'd be really useful to have someone who knows the real technical limitations on the Committee to rebut Clarke.

How to oversee unaudited actions of technical personnel

Finally, there's the problem of what to do with the 999 other Sysadmins and other technical personnel who have access to enormous amounts of

sensitive data but who are not currently overseen adequately.

This problem is probably not limited to Sysadmins — according to the Primary Order on the telecom dragnet, other technical personnel massage the database of all phone-based relationships in the US before the (audited actions of) analysts get it. Indeed, these technical personnel managed to misplace 3,032 dragnet files on their own server. We know this data didn't get destroyed in timely fashion, but since this access is not audited, we don't know what else happened to it.

And aside from the fact that so much recent reporting talks about how embarrassing NSA's security was, there's another reason why outside technologists should provide input on how to fix the problem. DOD has a serial problem with not addressing the threat posed by removable media, having refused to fix the problem after malware got introduced into DOD systems via a thumb drive in 2008 and after then Bradley Manning took entire databases on a Lady Gaga CD. Sure, I'm sure SAIC and Booz would love to get paid billions to advise DOD how to fix this problem, but wouldn't it be better to hear the advice of someone not trying to get rich off of it?

This is another are where, left to itself, DOD has historically been inclined to settle for ease of use rather than security (indeed, testimony at Manning's trial made it clear that was precisely the thought process). But DOD should at least hear an independent voice on this front, one with some technical knowledge about how DOD might fix this persistent problem.

The need for an outside is all the more urgent given Keith Alexander's stated preferred solution is to fire 90% of the Sysadmins (which seems to both misunderstand the problem and ignore some big problems with the proposed solution). It sounds like NSA wants to adopt a technical fix to the Sysadmin problem (they haven't acknowledged the problem with the other technical personnel yet). So it would be far

better to have a technical person to explain why
that's probably not going to work.