

THE DEAD-ENDERS INSIST THEIR ILLEGAL DRAGNET WAS AND IS NOT ONE

As I noted in my last post, seven Bush dead-enders plus KS Representative and House Intelligence member Mike Pompeo wrote a letter to ... someone ... pushing back against the RNC condemnation of the NSA dragnet. As I noted in that post, along with wagging their collective national security experience, the dead-enders used the same old stale tricks to deny that the dragnet surveils US person content.

The stale tricks, by now, are uninteresting. I find the list of the dead-enders (Eli Lake fleshed it out here) more so.

Here's the list of the dead-enders:

- Michael Hayden (NSA Director until 2005, DDNI 2005-2006, CIA Director 2006-2009)
- Mike Mukasey (AG 2007-2008)
- Michael Chertoff (DOJ Criminal AAG 2001-2003, DHS Secretary 2005-2009)
- Stewart Baker (Assistant DHS Secretary 2005-2009)
- Steven Bradbury (Acting OLC head 2005-2009)
- Eric Edelman (National Security lackey in OVP 2001-2003, Undersecretary of Defense for Policy 2005-2009)
- Ken Wainstein (AAG for National Security 2006-2008,

White House CT Czar 2008-2009)

Some of these we expect. Michael Hayden and Stewart Baker have been two of the main cheerleaders for NSA since the start of Snowden's leaks, and Michael Chertoff's firm (at which Hayden works) seems to be working under some kind of incentive to have as many of its top people defend the dragnet as well. Further, both Bradbury and Wainstein have testified to various entities along the way.

So in some senses, it's the usual gang of dead-enders.

But I find the collection of Michael Mukasey, Bradbury, and Wainstein, to be particularly interesting.

After all, they're the 3 names (and in Mukasey's case, authorizing signature) on this memo, which on January 3, 2008 authorized NSA to contact chain Internet (and phone) "metadata" of Americans collected via a variety of means, including FISA, broadly defined, which would include Protect America Act, and EO 12333 and potentially other means – but let's just assume it was collected legally, Bradbury and Wainstein say twice in the memo.

They implemented this change, in part, to make it easier to share "United States communications metadata" outside of the NSA, including with CIA, by name (though CIA made that request in 2004, before Hayden had moved over to CIA).

When implementing the change, they defined Internet "metadata" this way:

b) For electronic communications, "metadata" includes the information appearing on the "to," "from," "cc," and "bcc" lines of a standard e-mail or other electronic communication. For e-mail communications, the "from" line contains the e-mail address of the sender, and the "to," "cc," and "bcc"

lines contain the e-mail addresses of the recipients. "Metadata" also means (1) information about the Internet-protocol (IP) address of the computer from which an e-mail or other electronic communication was sent and, depending on the circumstances, the IP address of routers and servers on the Internet that have handled the communication during transmission; (2) the exchange of an IP address and e-mail address that occurs when a user logs into a web-based e-mail service; and (3) for certain logins to web-based e-mail accounts, inbox metadata that is transmitted to the user upon accessing the account. "Metadata" associated with electronic communications does not include information from the "subject" or "re" line of an e-mail or information from the body of an e-mail.

It includes IP (both sender and recipient, as well as interim), email address, inbox metadata which has reported to include content as well.

But let's take a step back and remember some timing.

In 2004 DOJ tried to clean up NSA's Internet metadata problem which legally implicated Michael Hayden directly (because he personally continued it after such time as DOJ said it was not legal). The solution was to get Colleen Kollar-Kotelly sign an opinion (dated July 14, 2004) approving the Internet collection as a Pen Register/Trap and Trace order. But she limited what categories of "metadata" could be collected, almost certainly to ensure the metadata in question was actually metadata to the telecoms collecting it.

Before the very first order expired – so before October 12, 2004 – the NSA already started breaking those rules. When they disclosed that violation, they provided some of the same excuses as when they disclosed the phone dragnet

violations in 2009: that the people who knew the rules didn't communicate them adequately to the people implementing the rules (see page 10ff of this order). As part of those disclosures, however, they falsely represented to the FISC that they had only collected the categories of "metadata" Kollar-Kotelly had approved.

The Court had specifically directed the government to explain whether this unauthorized collection involved the acquisition of information other than the approved Categories [redacted] Order at 7. In response, the Deputy Secretary of Defense [Paul Wolfowitz] stated that the "Director of NSA [Michael Hayden] has informed me that at no time did NSA collect any category of information ... other than the [redacted] categories of meta data" approved in the [redacted] Opinion, but also note that NSA's Inspector General [Joel Brenner] had not completed his assessment of this issue. [redacted] Decl. at 21.13 As discussed below, **this assurance turned out to be untrue.**

13 At a hearing on [redacted] Judge Kollar-Kotelly referred to this portion of the Deputy Secretary's declaration and asked: "Can we conclude that there wasn't content here?" [redacted] of NSA, replied, "There is not the physical possibility of our having [redacted] [my emphasis]

We don't know precisely what were the categories NSA had collected in defiance of Kollar-Kotelly's orders. But Julian Sanchez laid out why they'd be important in this post, in which he noted that because of the layered structure of the Internet, what is "metadata" for one layer of the Internet is legally content to another.

The crucial point here is that the detailed "metadata" for a particular

Internet communication, past the IP layer, typically wouldn't be processed or stored by the ISP in the way that phone numbers and other call data is stored by the phone company. From the ISP's perspective, all of that stuff is content. Depending on the particular communication, those further layers of metadata might be stored as business records by some other "third party" service provider, like Google—or they might not.

Either way, the acquisition of "metadata" other than IP addresses from an ISP or off the backbone is pretty clearly dissimilar from the collection of call data at issue in *Smith* in every important respect. It is not information conveyed to the Internet provider for the purpose of routing the communication; it is routing information conveyed through the provider just like any other content.

As the redacted exchange from John Bates' 2010 order above makes clear, the NSA told Kollar-Kotelly they were in compliance with the categories she laid out. She asked them specifically if they had collected content (which almost certainly refers to routing information that would not be metadata to the telecoms collecting it), and they assured her, at least twice, they weren't.

As Reggie Walton and John Bates would discover sometime around October 2009, not only had NSA in fact been collecting routing information that legally qualified as content, but they never stopped doing so.

Notwithstanding this and many similar prior representations [made on the fall 2009 reauthorization] there in fact had been systemic overcollection since [redacted]. On [redacted] the government provided written notice of yet another

form of substantial non-compliance discovered by NSA OGC on [redacted] this time involving the acquisition of information beyond the [redacted] authorized categories.

[snip]

This overcollection, **which had occurred continuously since the initial authorization** in [redacted] included the acquisition of [long redaction]. [my emphasis]

In March 2004, DOJ told Michael Hayden and others that routing information was content. In July 2004, Colleen Kollar-Kotelly told Michael Hayden and others that certain routing information was content they could not legally collect. Before October 2004, NSA “discovered” they were collecting content still, but Michael Hayden personally lied about doing so (though Paul Wolfowitz is probably the one who passed that onto the Court).

Then, soon after Mukasey replaced Alberto Gonzales in 2007, Wainstein and Bradbury got him to approve contact-chaining of “metadata” that used a definition of “metadata” that almost certainly constituted content under the guidelines laid out by Kollar-Kotelly.

And Michael Mukasey signed their authorization letter, without asking for written clarity as to where the data came from or whether it complied with FISC’s rulings on metadata (Bradbury and Wainstein used largely the same argument about metadata that Kollar-Kotelly had done).

Now, it may well be what Mukasey authorized was at least partly legal (assuming the initial collection was legal, as Bradbury and Wainstein would like you to do). Collecting metadata from FISA authorized collection – whether via individual warrant, PAA order, or stored communication under a physical search – would seem to permit the collection of metadata that counted as content, since FISA warrants and

orders are meant to authorize the collection of content (there are reasons to believe NSA still collects a lot of metadata under FAA orders). But if it were domestic upstream collection – perhaps transit collection – it would amount to the illegal dissemination of domestically collected US person content, which Bates would go on to tell the government was illegal in 2010. And as I've noted repeatedly, later in 2008, FISA Amendments Act arguably made such collection overseas illegal, absent a warrant, as well.

When this document first came out, we didn't know that FISC had told some of these same dead-enders that such collection – if collected domestically – was not legal. But it had, years earlier.