

DAVID KRIS OUTLINES THE INTERNET DRAGNET ELEPHANT

Way back on page 64 (of 67) of former Assistant Attorney General for National Security David Kris' paper "On the Bulk Collection of Tangible Things," he invokes the elephant metaphor the President used to promise more NSA disclosures on multiple programs.

What I'm going to be pushing the IC to do is rather than have a trunk come out here and leg come out there and a tail come out there, let's just put the whole elephant out there so people know exactly what they're looking at.

In keeping with the President's direction, the Intelligence Community has released many new details about the bulk telephony metadata collection program, as described above. In addition, as also noted above, the FISC itself has released significant new information. The key remaining question is whether there will be additional, authorized releases concerning intelligence activity that has not been subject to prior, unauthorized releases. [my emphasis]

Kris uses the President's elephant to ask whether they really will disclose their intelligence programs. He mentions just the phone dragnet (even though the Administration, in response to two FOIAs, also released information about their Section 702 upstream collection programs), even as he suggests the Administration might do well to admit to other programs before they are exposed by an Edward

Snowden leak.

Which is interesting, because Kris' paper – in spite of his title and in spite of that reference to the phone dragnet – is really about what the government has declassified (the phone dragnet) as well as what the government has left partly hidden (the Internet dragnet and broader phone dragnet).

Kris discusses the PATRIOT-authorized Internet dragnet along with the phone dragnet

Kris, after all, provides the following facts about the PATRIOT-authorized Internet dragnet, citing the named sources:

- Internet and telephony metadata was collected starting in 2001, until the 2004 hospital disagreement led to the former being moved to Pen Register/Trap & Trace authority in 2004, which was the first bulk order (“purported” NSA IG Report)
- One company – which the “purported” IG report makes clear was an Internet one and is probably Yahoo – did not participate in the illegal wiretap program (“purported” NSA IG Report)
- The Internet metadata collection ended in 2011 (an ODNI spokesperson in a Charlie Savage story)

Kris also points to four different Administration acknowledgements of the Internet metadata program. He refers to the 2009 and 2011 notice letters to Congress (though he focuses on

the phone dragnet language in them), and the James Clapper response to Wyden and 25 other Senators. Perhaps most interestingly, Kris notes that government witness(es) have confirmed the program and the use of PR/TT to authorize it...

At a July 17, 2013 hearing of the House Judiciary Committee, government witnesses confirmed the pen-trap bulk collection.

But unlike just about every other comment in a hearing cited in his paper, Kris doesn't quote the exchange, which went like this.

SUZAN DELBENE: The public also now knows that the telephone metadata collection is under Section 215, the Business Records provision of FISA, and that allows for the collection of tangible things. But we've also seen reports of a now-defunct program collecting email metadata. With regard to the email metadata program that is no longer being operated, can you confirm that the authority used to collect that data was also Section 215?

GEN. COLE: It was not. It was the Pen Register Trap and Trace Authority under FISA, which is slightly different, but it amounts to the same kind of thing. It does not involve any content. It is, again, only to and from. It doesn't involve, I believe, information about identity. It's just email addresses. So it's very similar, but not under the same provision.

REP. DELBENE: And could you have used Section 215 to collect that information?

GEN. COLE: It's hard to tell. I'd have to take a look at that.

The transcript from this hearing is up at the I Con the Record site, so it's unclear why Kris

didn't quote it. (Though note, I suspect Cole is wrong, and that the Internet dragnet did include identity, because the government used hybrid orders to get just that before PATRIOT reauthorization in 2006 included that in PR/TTs.) Yet it, like the other 3 references, makes it clear that you don't have to rely on "purported" documents the government won't acknowledge to show official confirmation of the PATRIOT-authorized Internet dragnet.

Kris discusses E.O. 12333 authorized phone and Internet dragnet

Then he goes further in outlining the Internet (and broader phone) dragnet. Citing the "purported" Ken Wainstein letter and the declassified (but still heavily redacted) End-to-End report, Kris suggests there's more than the PATRIOT-authorized Internet metadata the Administration has semi-admitted; there's broader collection on which the government does even more analysis (this is one instance where he makes it clear the government has used 2511(2)(f) to collect this other information, the significance of which I laid out here).

The government did not, of course, foreclose data mining, contact chaining,⁵⁴ or other analysis with respect to metadata responsive to queries,⁵⁵ or of metadata collected using methods or programs other than the FISC's bulk collection order under the FISA tangible things provision.⁵⁶

54 Contact-chaining involves the use of "computer algorithms. . . [to create] a chain of contacts linking communications and identifying additional telephone numbers, IP addresses, and e-mail addresses of intelligence interest." Memorandum for the Attorney General, from Kenneth L. Wainstein, Assistant Attorney General, November 20, 2007, at 2, available at <http://www.guardian.co.uk/world/interact>

ive/2013/jun/27/nsa-data-collectionjustice-department [hereinafter Wainstein Contact Chaining Memo]. As with the NSA Draft IG Report, the government has not acknowledged or declassified this memorandum, as it has for certain other unlawfully disclosed documents, and thus it is referred to here only as a document that is, in fact, available the Internet, but without any suggestion that it is or is not what it purports to be, or that any statements within it are accurate. The 215 Bulk Primary Order discusses contact chaining through queries. 215 Bulk Primary Order at 6.

55 See August 2013 FISC Order at 11-13.

56 Alternative methods of collection would include non-bulk FISA orders, or what prior NSA Directors in the past have referred to as “vacuum cleaner” surveillance outside the ambit of FISA, under Executive Order 12333 and its subordinate procedures, such as DOD 5240-1.R, and perhaps voluntary production if not otherwise prohibited by law. See NSA End-to-End Review at 15; August 2013 FISC Order at 10 n.10 (“The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court’s Orders.”); cf. 18 U.S.C. § 2511(2)(f) (“Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications

system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978"). A purported September 2006 letter from the Acting General Counsel of NSA to the Counsel for Intelligence Policy at DOJ, Attachment B to the Wainstein Contact Chaining Memo, notes that "NSA acquires this communications metadata . . . under Executive Order 12333. All of the communications metadata that NSA acquires under this authority should have at least one communicant outside the United States." For a discussion of "vacuum cleaner" surveillance, see Kris & Wilson, NSIP § 16:5 & nn.14, 31, § 16:12 & nn.16, 18, § 16:17. For a discussion of DOD 5240-1.R, see Kris & Wilson, NSIP §§ 2:7-2:9, Appendix J. The purported Wainstein Contact Chaining Memo discusses such contact chaining with respect to the "large amount of communications metadata," including metadata associated with persons in the United States, contained in NSA's databases. Wainstein Contact Chaining Memo at 3. The 215 Bulk Primary Order states that the FISA "Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata." 215 Bulk Primary Order at 13 n.15.

Through this very contorted set of footnotes, Kris makes it clear that the dragnet is about far more than just PATRIOT-authorized phone and Internet dragnets. He shows us at least hints of the trunk of the elephant of Internet dragnet that the Administration has thus far been unwilling to reveal on its own, even while both the WSJ and NYT have disclosed parts of it.

Indeed, Kris' efforts to discuss this may well be so contorted because (as he notes on the

first page of the paper) it has been subject to “an iterative process of prepublication review.”

To understand why those contortions are so fascinating, remember Kris’ history.

Kris oversaw efforts to clean up the phone and (almost certainly) Internet dragnets

Kris served in a top national security role in Bush’s DOJ, but was not read into Cheney’s illegal wiretap program (indeed, Kris successfully lobbied Congress for changes to FISA at the same time Cheney chose not to ask for changes that would have authorized his illegal program). Then, after he left government, he helped DOJ shore up their public case for the illegal program, but afterwards issued a paper critical of one of Bush’s central claims, that the AUMF authorized overriding FISA. Remember, though: that paper addressed only the publicly admitted part of the illegal program – the content collection. It didn’t address metadata, which is not electronic surveillance, and therefore not subject to the same objections Kris raised.

Under Obama, Kris returned to DOJ. He was confirmed to be AAG of the National Security Division on March 25, 2009, resigned on January 13, 2011, and left on March 4, 2011. Rather than following the career path of his predecessors (several of whom moved to the White House counterterrorism czar position), Kris moved all the way across the country to serve as General Counsel for a patent troll.

Kris’ timing in the Obama DOJ meant he took over NSD not long after DOJ started responding in earnest to Reggie Walton’s concerns about the phone dragnet program. Kris would almost certainly have overseen DOJ’s side of the process of working through the phone dragnet problems (which is why I suggested he’d be intimately familiar with the End-to-End review he cites to talk about the broader phone dragnet). In September 2009, one of his attorneys at NSD alerted the FISC of additional

violations the NSA did not reveal of its own accord. Kris would also have overseen cleaning up the second misrepresentation the government made to FISC, which almost certainly pertains to the Internet dragnet. And he would have left not long before DOJ confessed to the third of three misrepresentations to the FISA Court, that pertaining to upstream collection (the first declaration in the FISA Amendments Act reapplication process was April 20, 2011), though he was gone before the tedious process of working through that misrepresentation. And less than a year after he left, the government stopped the PATRIOT-authorized Internet dragnet.

Which is another way of saying Kris knows this stuff, especially the problems with both the phone and Internet dragnets, and made real efforts to clean up what were actually problems leftover from the illegal program.

Kris' support for these programs is somewhat ambivalent

Which is why those declaring "major victory" about this paper might want to read more closely. Because Kris' support for the dragnets is somewhat ambivalent.

Even in his case citations supporting the dragnets, Kris seems to be making a different argument than the flunkies who wrote the Administration White Paper on the phone dragnet. Whereas the Administration argues for almost unlimited application of "relevance," Kris' readings of some of the same case citations actually support the practice of pre-filtering where possible (though he supports the Administration claims that pre-filtering is not possible for phone records).

The question, then, was whether the appropriate "category of materials" to be assessed was "the information-storage devices demanded, or . . . the documents contained within them."⁸⁸ The court held that it was the documents, in part because "the government has acknowledged

that a 'key word' search of the information stored on the devices would reveal 'which of the documents are likely to be relevant to the grand jury's investigation,'" but still tried to insist on receiving all of the storage devices in full.⁸⁹ Judge Mukasey's decision seems to depend in substantial part on the idea that the government had at its disposal a feasible method of pre-filtering the information to be collected—a concession that the government has not made with respect to its bulk collection of telephony metadata.

This is, after all, what happens to the 75% of US Internet traffic accessed via telecom pre-filtering, as described by the WSJ and not actually denied by ODNI which, however, doesn't get mentioned in Kris' paper. Kris is making a better case for NSA to get pre-filtered dragnet data than he is for the phone dragnet as it currently exists.

And, as I'm sure a lot of lawyers will point out, even where Kris makes a "case" to support the dragnet, it's rather thin. For example, on both the issues of using Section 215 to collect data for NSA rather than FBI and the ongoing nature of the production, Kris provides almost no statutory support for his argument dismissing these problems. As such, raising them serves more as a roadmap for challenging the program, not a defense of it. In fact, I think these problems identified by Kris actually explain DOJ's request to delay its filing in the ACLU Section 215 FOIA – so it can account for Kris' arguments.

Moreover, at two points in his paper, Kris suggests the original bulk collection decisions may be fairly shoddy. He suggests FISC may have approved it in 2006 not because the legal case was great, but because it was preferable to have the bulk collection under the supervision of the FISC rather than not.

More broadly, it is important to consider the context in which the FISA Court initially approved the bulk collection. Unverified media reports (discussed above) state that bulk telephony metadata collection was occurring before May 2006; even if that is not the case, perhaps such collection could have occurred at that time based on voluntary cooperation from the telecommunications providers. If so, the practical question before the FISC in 2006 was not whether the collection should occur, but whether it should occur under judicial standards and supervision, or unilaterally under the authority of the Executive Branch.

And as part of his (flawed) argument that Congressional reauthorization of these programs makes them legal, Kris suggests the original decision may have been erroneous.

The briefings and other historical evidence raise the question whether Congress's repeated reauthorization of the tangible things provision effectively incorporates the FISC's interpretation of the law, at least as to the authorized scope of collection, such that even if it had been erroneous when first issued, it is now—by definition—correct. [my emphasis]

And all of that is well before Kris' 3 mentions of the government's reliance on 18 U.S.C. § 2511(2)(f). I'm still trying to figure out whether he is exposing this use, or trying to legitimize it. But Kris may well be saying that the government can (and does) move things under 12333 and 2511(2)(f) when they get problematic under FISC oversight (and if he's not, that's a clear implication of his paper).

(Note, I'm finishing this up while watching the Senate Judiciary Committee, and Keith Alexander

just admitted to this 12333 metadata program, though he keeps retreating to talking about the FISC-supervised program.)

As inklings of the program have been exposed, it becomes clear that the last four months of Administration damage control have focused on falsely claiming that the only dragnet is the relatively closely-supervised phone dragnet. That's not true (and it's also not true that only counterterrorism targets are investigated under the dragnet).

Kris' paper hints at that. He hints at that elephant – the massive metadata dragnet – the Administration is still hiding under the bed.

It's what we do with the elephant that is particularly pressing.