JAMES CLAPPER CLAIMS PUBLICLY ACKNOWLEDGED DETAILS ARE STATE SECRETS WHILE BOASTING OF TRANSPARENCY

Between documents leaked by Edward Snowden, official court submissions, and official public statements, we know at least the following about the surveillance system set up after 9/11 and maintained virtually intact to this day:

- Around of 8-14% of the content collected under Bush's illegal program was domestic content (page 15 of the NSA IG Report says this constituted 8% of all the illegal wiretap targets but the percentage works out to be higher)
- Some of the content collected via ongoing upstream collection currently includes intentionally-collected domestic content (NSA refuses to count this, even for the FISA Court)
- Bush's illegal wiretap program targeted Iraqi Intelligence Service targets, as well as targets

affiliated with al Qaeda and its associates (see page 8)

- NSA uses the phone metadata program with Iranian targets, as well as targets affiliated with al Qaeda and its associates
- Both the illegal wiretap program and the Internet dragnet authorized under Pen Register/Trap and Trace in 2004 collected information that (because of the way TCP/IP works) would be legally content if treated as electronic surveillance
- The NSA still conducts an Internet dragnet via collection overseas, which not only would permit the metadata-as-content collection, but would permit far more collection on US persons; that collection is seamlessly linked to the domestic dragnet collection
- NSA uses the dragnets to decide which of content the telecoms have briefly indiscriminately collected to read

> That is, the surveillance system is not so much discrete metadata programs and content programs directed overseas, directed exclusively against al Qaeda or even terrorists. Rather, it is a system in which network analysis plays a central role in selecting which collected content to

read. That content includes entirely domestic communication. And targets of the system have not always been — and were not as recently as June — limited to terrorists.

These details of the surveillance system — along with the fact that AT&T and Verizon played the crucial role of collecting content and "metadata" off domestic switches — are among the details James "Least Untruthful" Clapper, with backup from acting Deputy Director of NSA Frances Fleisch, declared to still be state secrets on Friday, in spite of their public (and in many cases, official) acknowledgement.

In doing so, they are attempting to end the last remaining lawsuits for illegal wiretapping dating to 2006 by prohibiting discussion of the central issue at hand: the government has repeatedly and fairly consistently collected the content of US persons from within the US, at times without even the justification of terrorism. (For more background on Jewel v. AT&T, see here.)

Here's how Clapper, with a nod to Fleisch, lays out the rebuttal of the Jewel plaintiffs.

> the NSA's collection of the content of communications under the TSP was directed at international communications in which a participant was reasonably believed to be associated with al-Qa'ida or an affiliated organization. Thus, as the U.S. Government has previously stated, plaintiff's allegation that the NSA has indiscriminately collected the content of millions of communications sent or received by people inside the United States after September 11, 2001, under the TSP is false.

There are several weasel parts of this claim.

The "Terrorist Surveillance Program" and the "Other Target Surveillance Program"

First, to make this claim, Clapper (and Fleisch)

revert to use of “Terrorist Surveillance Program,” a term invented to segment off the part of the larger illegal wiretap program that George Bush was willing to confess to in December 2005, that involving international communications with a suspected al Qaeda figure. But as Fleisch admits — but doesn’t explain — at ¶20, the TSP is just a subset of the larger Presidential Surveillance Program. As I’ve noted above, we know the system was used and is currently used to target entities that are agents of states, not terrorist organizations. And Clapper’s language suggests it is used with both “other foreign terrorist organizations” and to identify “many other threats.”

> …and other foreign terrorist organizations to the United States
>
> [snip]
>
> to the extent classified information about the al-Qa’ida threat, from September 11, 2001 to the present, or the many other threats facing the United States,

Given the evidence that the program may (or may have) extend beyond even the Iranian and Iraqi targets the government has deemed “terrorists” so as to include them in this program, Jewel’s plaintiffs might be able to argue it could include normal dissent.

The Internet metadata that is really content

Then the government hides details that would make it clear that both under Bush and Obama, NSA illegally collected US person content in the name of collecting “metadata.”

The first tell here is how Clapper refers to the “metadata” collected under Bush (this carries over into the I Con’s announcement of this declassification).

> President Bush authorized the NSA to collect (1) the contents of certain

> international communications, a program that was later referred to and publicly acknowledged by President Bush as the Terrorist Surveillance Program (TSP), and (2) telephony and Internet non-content information (referred to as "metadata") in bulk, subject to various conditions. [my emphasis]

While his reference varies, the emphasis on "non-content information (referred to as 'metadata')" suggests they're using a potentially uncertain definition of metadata.

This likely derives from the government's definition of content here. Both Clapper (footnote 1) and Fleisch (footnotes 4 and 11) note their discussion of the Internet "metadata" program defines content as defined under the pen register part of FISA. Here's Fleisch:

> The term "content" is used herein to refer to the substance, meaning, or purport of a communication, as defined in 18 U.S.C. § 2510(8), as distinguished from the type of addressing or routing information referred to herein as "metadata."

While they claim to be using "meaning" to distinguish from "metadata," both are also implicitly distinguishing this definition of content used in the pen register statute from that used for electronic surveillance, which is,

> "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

At one level, this is just tautological game-playing. The method the NSA used to collect the domestic Internet dragnet until December 2011

was exactly the same as it used for the Section 702 upstream collection, collection, with some filtering, directly from AT&T and Verizon's switches; there is nothing in the method that distinguishes the Internet dragnet from what NSA treats as electronic surveillance of Internet content. So to define one object of collection as metadata and the other as content, they simply apply different definitions of content to them.

Moreover, there is long-standing legal awareness of this problem. Colleen Kollar-Kotelly relied on the pen register definition on page 6 of the original dragnet opinion. But with it, she required that collection be limited to certain kinds of metadata, a requirement that we know NSA violated from the very start.

John Bates laid out the problems with adopting the pen register definition generally and therefore its definition of content specifically on pages 26 and following of his opinion authorizing the resumption of the Internet dragnet. That problem appears to pertain to the fact that the NSA was claiming that PR/TT allowed it to collect "dialing, routing, addressing, or signaling information" (DRAS), whether or not it was content, and data that was not content as defined under the pen register statute. Bates judged (see page 30 and following) that Congress intended to authorize DRAS collection only if it was not content. Since the Internet uses nested addressing, and subordinate addresses would be treated as content to the higher level routing entities, the government was effectively collecting metadata that was content (again, see Julian Sanchez' explanation of why this is significant from a legal standpoint).

But here we are, just 3 years after Bates described all this in a court ruling (and 2 years after he repeated some of the same analysis in another court ruling), and the government is making the argument that metadata collected using the same method as content is

not content because it doesn't meet the "content" definition of the statute that doesn't allow you to collect content, even while it does meet the "content" definition of the statute that allows you to collect content.

Oh, and by the way, the collection of US person Internet metadata-that-is-also-content still goes on overseas; the government's assertion that that collection doesn't go on anymore makes it clear it doesn't go on under the FISA pen register statute, without ruling out such collection under other authorities.

> In December 2011 , the U.S. Government decided not to seek re-authorization of the bulk collection of lnternet metadata under section 402.

Which is quite different from saying — as they have in unsworn statements — that they've shut down the program entirely.

The metadata that leads to the content

Finally, Clapper and Fleisch impose silence over the relationship between this metadata and content, declaring state secrets over both the scope of the TSP (and therefore implicitly, the PSP) and 702 collection, as well as,

> any other information related to demonstrating that the NSA has not otherwise engaged in the content-surveillance dragnet that the plaintiffs allege

Nowhere in their declarations is there any language akin to the language Teresa Shea, NSA Director of Signals Intelligence Directorate, used just a month ago in the Larry Klayman suit.

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the

> NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

To be fair, both of these passages use wonderfully vague language. "Content-surveillance dragnet" is something distinct from "content dragnet," the latter of which might refer to the collection but not review of content. And "content analysis" likewise assumes the content already got collected.

So both the effort to avoid describing and the effort to describe how the metadata ties directly into selecting which already-collected content to read gloss over that "already-collected" assumption (page 16 and following of the NSA IG Report describes some of this, and makes it clear the telecoms are using the metadata to pull the content for further analysis).

The thing is, the government likely has reason to be mighty uncertain about the legal status of this (or, even more likely, mighty certain but unhappy). While it is likely that the US person content systematically read using this system does not include the plaintiffs, the reason it doesn't is because the telecoms have already collected the plaintiffs' metadata (which, in

the case of their Internet data, is also legally content) and because they've briefly held their content while they scan it against selected metadata identifiers selected by analyzing all metadata identifiers, including their own.

They might win an argument that this collection was not indiscriminate, but to win it, they'd have to reveal the many places in the process where they had violated wiretap laws.

Thus, Clapper is instead using Bush and Obama's favorite strategy of declaring evidence of crime a state secret. All the while boasting of his own transparency in declassifying one more tiny chunk of Bush's illegal program.