THE AUGUST 20, 2008 CORRELATIONS OPINION

On August 18, 2008, the government described to the FISA
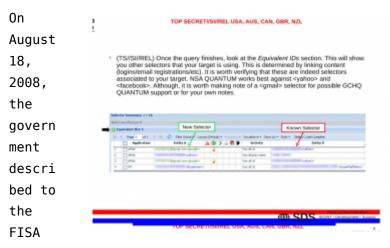

Court how it used a particular tool to establish correlations between identifiers. (see page 12)

> A description of how [name of correlations tool] is used to correlate [description of scope of metadata included] was included in the government's 18 August 2008 filing to the FISA Court,

On August 20, 2008, the FISC issued a supplemental opinion approving the use of "a specific intelligence method in the conduct of queries (term "searches") of telephony metadata or call detail records obtained pursuant to the FISC's orders under the BR FISA program." The government claims that it cannot release any part of that August 20, 2008 opinion, which given the timing (which closely tracks with the timing of other submissions and approvals before the FISC) and the reference to both telephony metadata and call detail records almost certainly approves the use of the dragnet — and probably not just the phone dragnet — to establish correlations between a target's multiple communications identifiers.

As ODNI's Jennifer Hudson described in a declaration in the EFF suit, the government maintains that it cannot release this opinion,

in spite of (or likely because of) ample
description of the correlations function
elsewhere in declassified documents.

> The opinion is only six pages in length
> and the specific intelligence method is
> discussed at great length in every
> paragraph of this opinion, including the
> title. Upon review of this opinion, I
> have determined that there is no
> meaningful, segregable, non-exempt
> information that can be released to the
> plaintiff as the entire opinion focuses
> on this intelligence method. Even if the
> name of the intelligence method was
> redacted, the method itself could be
> deduced, given other information that
> the DNI has declassified pursuant to the
> President's transparency initiative and
> the sophistication of our Nation's
> adversaries **[Ed: did she just call me an
> "adversary"?!?]** and foreign intelligence
> services.
>
> [snip]
>
> The intelligence method is used to
> conduct queries of the bulk metadata,
> and if NSA were no longer able to use
> this method because it had been
> compromised, NSA's ability to analyze
> bulk metadata would itself be
> compromised. A lost or reduced ability
> to detect communications chains that
> link to identifiers associated with
> known and suspected terrorist
> operatives, which can lead to the
> identification of previously unknown
> persons of interest in support of anti-
> terrorism efforts both within the United
> States and abroad, would greatly impact
> the effectiveness of this program as
> there is no way to know in advance which
> numbers will be responsive to the
> authorized queries.

ACLU's snazzy new searchable database shows that

this correlations function was discussed in at least three of the officially released documents thus far: in the June 25, 2009 End-to-End Review, in a June 29, 2009 Notice to the House Intelligence Committee, and in the August 19, 2009 filing submitting the End-to-End Review to the FISC.

In addition to making it clear this practice was explained to the FISC just before the Supplemental Opinion in question, these documents also describe a bit about the practice.

They define what a correlated address is (and note, this passage, as well as other passages, do not limit correlations to telephone metadata — indeed, the use of "address" suggests correlations include Internet identifiers).

> The analysis of SIGINT relies on many techniques to more fully understand the data. One technique commonly used is correlated selectors. A communications address, or selector, is considered correlated with other communications addresses when each additional address is shown to identify the same communicant as the original address.

They describe how the NSA establishes correlations via many means, but primarily through one particular database.

> NSA obtained [redacted] correlations from a variety of sources to include Intelligence Community reporting, but the tool that the analysts authorized to query the BR FISA metadata primarily used to make correlations is called [redacted].
>
> [redacted] — a database that holds correlations [redacted] between identifiers of interest, to include results from [redacted] was the primary means by which [redacted] correlated identifiers were used to query the BR

> FISA metadata.

They make clear that NSA treated all correlated identifiers as RAS approved so long as one identifier from that user was RAS approved.

> In other words, if there: was a successful RAS determination made on any one of the selectors in the correlation, all were considered .AS-a. ,)roved for purposes of the query because they were all associated with the same [redacted] account

And they reveal that until February 6, 2009, this tool provided "automated correlation results to BR FISA-authorized analysts." While the practice was shut down in February 2009, the filings make clear NSA intended to get the automated correlation functions working again, and Hudson's declaration protecting an ongoing intelligence method (assuming the August 20, 2008 opinion does treat correlations) suggests they have subsequently done so.

When this language about correlations first got released, it seemed it extended only so far as the practice — also used in AT&T's Hemisphere program — of matching call circles and patterns across phones to identify new "burner" phones adopted by the same user. That is, it seemed to be limited to a known law enforcement approach to deal with the ability to switch phones quickly.

But both discussions of the things included among dragnet identifiers — including calling card numbers, handset and SIM card IDs — as well as slides released in stories on NSA and GCHQ's hacking operations (see above) make it clear NSA maps correlations very broadly, including multiple online platforms and cookies. Remember, too, that NSA analysts access contact chaining for both phone and Internet metadata from the same interface, suggesting they may be able to contact chain across content type. Indeed, NSA

presentations describe how the advent of smart phones completely breaks down the distinction between phone and Internet metadata.

In addition to mapping contact chains and identifying traffic patterns NSA can hack, this correlations process almost certainly serves as the glue in the dossiers of people NSA creates of individual targets (this likely only happens via contact-chaining after query records are dumped into the corporate store).

Now it's unclear how much of this Internet correlation the phone dragnet immediately taps into. And my assertion that the August 20, 2008 opinion approved the use of correlations is based solely on … temporal correlation. Yet it seems that ODNI's unwillingness to release this opinion serves to hide a scope not revealed in the discussions of correlations already released.

Which is sort or ridiculous, because far more detail on correlations have been released elsewhere.