

THE FOREIGN METADATA PROBLEM

In this post, I argued that a likely explanation for the NSA's limits on collecting domestic cell phone data stem from a decision Verizon made in 2009 to stop participating in an FBI call records program. I'm not sure if I'm right about the cause (I know I'm not right about the timing), but I based part of my argument on how the FISA Court resolved a problem with telecoms turning over foreign data in 2009. And that resolution definitely indicates there's something different about the way Verizon produces dragnet data from how AT&T does (Sprint is probably a third case, but not as important for these purposes).

Let me be clear: Verizon was not the only telecom to have the problem. It affected at least one other telecom; I believe it may have affected all of them. But the FISC resolved it differently with Verizon, which I believe shows that Verizon complies with the Section 215 orders in different fashion than AT&T and Sprint.

The problem was first identified when, in May 2009, Verizon informed the NSA it had been including foreign-to-foreign records in the data it provided to the NSA. Here's how David Kris explained it in his report accompanying the phone dragnet end to end report.

NSA advised that for the first time, in May 2009, [redacted-Verizon] stated it produced foreign-to-foreign record pursuant to the Orders. [redacted-Verizon] stopped its production of this set of foreign-to-foreign records on May 29, 2009, after service of the Secondary Order in BR 09-06, which carves out foreign-to-foreign records from the description of records to be produced. (19)

In an accompanying declaration Keith Alexander provided more detail.

In May 2009, during a discussion between NSA and [redacted-Verizon] regarding the production of metadata, a [redacted-Verizon] representative stated that [redacted] produced the records [redacted] pursuant to the BR FISA Orders. This was the first indication that NSA had ever received from [redacted-Verizon] of its contrary understanding. At the May 28, 2009, hearing in docket number BR 09-06, the government informed the Court of [redacted redacted]. To address the issue, based on the government's proposal, the Court issued a Secondary Order to [redacted] in docket number BR 09-06 that expressly excluded foreign-to-foreign call detail records from the scope of records to be produced. On May 29, 2009, upon service of the Secondary Order in docket number BR 09-06, [redacted-Verizon] ceased providing foreign-to-foreign records [redacted].
(42/PDF67)

Almost every dragnet order since that May 29, 2009 one has broken its production order out into two subparagraphs to reflect this change.

(1) (A) The Custodians of Records [redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"¹ created by [redacted]
[redacted]

(B) The Custodian of Records of [redacted]
[redacted]
[redacted]
[redacted] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily

We can be virtually certain that Verizon is this provider, because the Verizon secondary order leaked by Edward Snowden includes the language

excluding foreign-to-foreign data. That long redaction likely hides Verizon's full name under this program, "Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon"), which is the name initially used in the secondary order.

Additionally, ODNI originally released the January 20, 2011 primary order with the paragraph that clarifies this with Verizon's name unredacted. The paragraph remains in the dragnet orders, even after Verizon and Vodafone split earlier this year (though if the split affected this issue, they may have hidden the fact by retaining the paragraph, given that they're now anticipating declassification of the orders).

Less than a month after this incident, on June 25, the NSA finished its End-to-End report, which reported just the Verizon issue. Sometime between then and July 9, the FISC appears to have realized one of the other providers had a similar problem. The July 9, 2009 dragnet order, in the only exception I know to the two-part production order, looked like this:

(1) The Custodians of Records of (b)(1) and (b)(3)
(b)(1) and (b)(3)
(b)(1) and (b)(3) shall produce to NSA upon
service of the appropriate secondary order, and continue
production on an ongoing daily basis thereafter for the duration
of this Order, unless otherwise ordered by the Court, an
electronic copy of the following tangible things: all call
detail records or "telephony metadata"¹ created by (b)(1) and (b)(3)
(b)(1) and (b)(3) for communications (i) between the United States and
abroad; or (ii) wholly within the United States, including local
telephone calls. (b)(1) and (b)(3)
(b)(1) and (b)(3)

The production order is to plural custodians of records, meaning at least two providers must be named. But it applies the Verizon rules to all of the named providers.

The order also requires an explanation for inclusion of the foreign-to-foreign records (see the bullet at 16-17). It is redacted in the released order but the DOJ submission (see page 6) shows that Judge Walton ordered,

a full explanation of the extent to which NSA has acquired call detail records of foreign-to-foreign communications from [redacted—too long to just be Verizon] pursuant to orders of the FISC, and whether the NSA's storage, handling, and dissemination of information in those records, or derived therefrom, complied with the Court's orders;

The September 3, 2009 order reverts to the two-paragraph structure. But it also orders retroactive production from one of the providers (AT&T or Sprint, probably the latter based on redaction length) named in the first paragraph (I first wrote about this here).

In addition, the Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate Secondary Order an electronic copy of the same tangible things created by [redacted] for the period from 5:11 p.m. on July 9, 2009 to the date of this Order, to the extent those records still exist.

And adds a requirement that NSA report on any significant changes in reapplications, including on any changes to how the government obtains the data from carriers.

Any application to renew or reinstate the authority granted herein shall include a report describing: (1) the queries made since the end of the reporting period of the last report filed with the Court; (ii) the manner in which NSA applied the procedures set forth in paragraph (3)C above; and (iii)

any proposed changes in the way in which the call detail records would be received from the carriers and any significant changes to the systems NSA uses to receive, store, process, and disseminate BR metadata. [my emphasis]

The DOJ report provides further evidence that at least one other provider provided foreign-to-foreign records. When Kris introduces this problem (see page 18), he references a three part discussion in Alexander's declaration.

NSA has acquired records of foreign-to-foreign communications from [REDACTED]
[REDACTED] With the possible exception of certain foreign-to-foreign records produced by [REDACTED]
[REDACTED] NSA has stored, handled and disseminated foreign-to-foreign records produced pursuant to the Orders in accordance with the terms of the Orders. See Ex. A at 39-44 [REDACTED] 44-46 [REDACTED]
[REDACTED] and 46-47 [REDACTED] (TS//SI//NF)

You can see the heading for the third provider on page 46/PDF 71 of the Alexander declaration.

So the report appears to have commented on all three providers. The problem clearly affected two of them.

But FISC only retains the clarification for Verizon.

As I said, I appear to be wrong about the timing of this. I had suggested it was tied to Verizon deciding not to reup its contract under the FBI phone program in 2009. That almost certainly had to have happened (as Charlie Savage noted to me via Twitter, the Exigent Letter IG Report was focused on AT&T, MCI, and Verizon, and one of the latter two, which means basically one part of Verizon, backed out).

But the End-to-End Report makes it clear Verizon first started turning over this data in January 2007.

This foreign-to-foreign metadata started coming into NSA in January 2007. (15)

There was not even a dragnet order signed in January 2007, so it can't be tied primarily to

the phone dragnet. It also preceded the end of the on-site phone provider program (which ended in December 2007) and even the release of the first NSL IG Report in March 2007, which led the providers to get squirrely (see page 191 for these dates).

The details regarding the potential problems with Verizon's provision of foreign-to-foreign records suggests this may have something to do with upstream production (Verizon had been providing upstream records to the NSA for years, but it only came under the oversight of the FISC in January 2007).

Furthermore, because the records are records of foreign-to-foreign communications, almost all of them do not concern the communications of U.S. persons. To the extent any of the records concern the communications of U.S. persons, such communications would be afforded the same protections as any other U.S. person communication [redacted] authorities. Id. at 43. (19)

[snip]

almost all of them concern the communications of non-U.S. persons located outside the United States. If NSA were to find that any of the records concerned U.S. persons, their dissemination would be governed by the terms of USSID 18 which are the procedures established pursuant to E.O. 12333, as amended. (68)

The discussion of records that might "concern the communications" sounds like an "about" search (though I'm not sure *of what*).

All that said, AT&T should have had the same upstream "about" obligations starting in January 2007 that Verizon did. I suspect (based on my guess that Sprint is the production that got shut down) the order in the July 9, 2009 order

is the only instruction they ever got to stop providing foreign-to-foreign records. Yet FISC felt the need – still feels the need – to keep that explicit order to Verizon in every single primary order.

Mind you, all this shows that Verizon was able to shut down the foreign production immediately, on the same day. So it's clear they can shut down certain kinds of production.

All this seems to suggest that – in addition to at least some part of Verizon withdrawing from the FBI's records program, and to Verizon not retaining records for the same length of time AT&T does – Verizon also produces phone dragnet data differently than AT&T does.