NSA'S DATA RETENTION ODDITIES

NSA's defenders are enjoying this one: WSJ says that NSA may temporarily have to expand the phone dragnet (it really means retain more data) because of all the lawsuits to end it.

> A number of government lawyers involved in lawsuits over the NSA phone-records program believe federal-court rules on preserving evidence related to lawsuits require the agency to stop routinely destroying older phone records, according to people familiar with the discussions. As a result, the government would expand the database beyond its original intent, at least while the lawsuits are active.
>
> No final decision has been made to preserve the data, officials said, and one official said that even if a decision is made to retain the information, it would be held only for the purpose of litigation and not be subject to searches.

There is actually a precedent for this. In 2009, as NSA was trying to clean up its alert list and other violations, it told the FISA Court it might not be able destroy all the alert notices because of ongoing litigation.

> With respect to the alert process, after this compliance matter surfaced, NSA identified and eliminated analyst access to all alerts that were generated from the comparison of non-RAS approved identifiers against the incoming BR FISA material. The only individuals who retain continued access to this class of alerts are the Technical Director for NSA's Homeland Security Analysis Center ("HSAC") and two system developers assigned to HSAC. From a technical

> standpoint, NSA believes it could purge copies of any alerts that were generated from comparisons of the incoming BR FISA information against non-RAS approved identifiers on the alert list. However, the Agency, in consultation with DoJ, would need to determine whether such action would conflict with a data preservation Order the Agency has received in an ongoing litigation matter.

Though I can't think of any follow-up confirming whether NSA believed this massive violation should or should not be retained in light of ongoing litigation.

As EFF's Cindy Cohn notes in the WSJ article, if NSA should be retaining data, it should date back to when a judge first issued a preservation order.

> Cindy Cohn, legal director at the Electronic Frontier Foundation, which also is suing over the program, said the government should save the phone records, as long as they aren't still searchable under the program. "If they're destroying evidence, that would be a crime," she said.
>
> Ms. Cohn also questioned why the government was only now considering this move, even though the EFF filed a lawsuit over NSA data collection in 2008.
>
> In that case, a judge ordered evidence preserved related to claims brought by AT&Tcustomers. What the government is considering now is far broader.

Though when I saw reference to the litigation in the 2009 filing, I wondered whether it might be either the al-Haramain suit or one of the dragnet suits, potentially including EFF's suit.

Here's what confuses me about all this data retention business.

If the NSA is so cautious about retaining evidence in case of a potential crime, then why did it just blast away the 3,000 files of phone dragnet information they found stashed on a random server, which may or may not have been mingled in with STELLAR WIND data it found in 2012? Here's how PCLOB describes the data and its destruction, which differs in some ways from the way NSA described it to itself internally.

> In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit.

According to the NSA, they didn't know how or why or when the data ended up where it wasn't supposed to be or even if it had really been retained past the age-off date.

Heck, those 3,000 files potentially mixed up with STELLAR WIND data seem like precisely the kind of thing EFF's Jewel suit might need to access.

But it's all gone!

One final detail. Here's how WSJ says the system currently ages off data.

> As the NSA program currently works, the database holds about five years of data,

> according to officials and some declassified court opinions. About twice a year, any call record more than five years old is purged from the system, officials said.

This is not how witnesses have consistently described the age-off system. It adds up to 6 months on the age-off, in what appears to be non-compliance with the unredacted parts of the phone dragnet orders.

Update: Adding one more thing. WSJ suggests NSA may have to keep the data because it might help some of the plaintiffs get standing. The only way that's true is if NSA stopped getting Verizon cell data from Verizon starting in 2009.

For most of the plaintiffs, standing should be no problem They're Verizon Business Service customers. But Larry Klayman is just a cell phone customer. A 5-year age off (ignoring the semi-annual purge detail) would mean they'd be getting rid of data collected in February 2009, just as NSA was working through the violations and before the May 29, 2009 order for Verizon to stop handing over its foreign data (also before Reggie Walton shut down Verizon production for a 3 month period later in 2009). I'm not sure I buy all that, but it is the only way standing might depend on data retention.