NSA — CONTINUALLY VIOLATING FISA SINCE 2004

Last year, I did a report that catalogued all the times NSA had violated FISA since the Stellar Wind phone dragnet got moved under FISA in 2004. There were the five different practices deemed violations of 1809(a)(2), which prohibits the use of any data that was illegally collected.

> From 2004 until 2009, in spite of twice quarterly Office of General Counsel spot checks imposed to prevent it, "'[v]irtually every PR/TT record' generated [by the bulk Internet metadata program] included some data that had not been authorized for collection." 3
>
> From 2007 until 2011, NSA collected entirely domestic and untargeted communications as part of Multiple Communication Transaction bundles without restricting access to the unrelated communications. 4
>
> In June 2010, NSA admitted it had improperly retained Title I data in a management system that the court had deemed an overcollection; in May 2011, FISC found this retention problematic under 1809(a)(2). The government even argued that prohibitions 5 on using unlawfully collected information "only applied to interceptions authorized by the Court and did not apply to the fruits of unlawful surveillance."
>
> From 2011 to 2016, NSA retained Section 702 overcollection in its management systems, in spite of the 2011 FISC retention precedent ruling such retention a violation of 1809(a)(2). 7
>
> In 2013, NSA discovered its post-tasking

> checks to ensure targeted phones had not roamed into the United States had not functioned properly for some redacted period of time (possibly dating back to 2008), meaning some of the telephone collection from that period may have been collected on individuals located inside the United States in violation of 702. 8

In addition to those, NSA had continued to conduct back door searches of data collected using upstream 702 collection even after John Bates prohibited the practice in 2011.

> Because upstream collection foreseeably results in the collection of domestic communications, when John Bates first permitted searches of 702 data using US person identifiers in late 2011, he prohibited such searches on upstream data, for fear it would amount to using 702 for domestic surveillance. Yet NSA starting disclosing "many" such violations as early as 2013. 9
>
> As NSA's compliance organizations started looking more closely in 2015 and 2016, they discovered the NSA was even conducting such searches in systems "that do not interface with NSA's query audit system," raising questions about their ability to oversee US person queries 10 more generally. NSA discovered that some data obtained using upstream collection had been mislabeled as PRISM collection, meaning it would get no special treatment. With one tool used 11 to conduct queries of Americans located overseas, NSA experienced an 85% noncompliance rate. 12

While Rosemary Collyer (who is the worst presiding FISA Judge ever) didn't deem that a violation of 1809(a)(2) — meaning NSA didn't have to segregate and destroy andy data

collected improperly — it still violated the minimization procedures that control 702 collection.

So between 2004 and 2016, NSA was always breaking the rules of FISA in one way or another.

And we can now extend that timeline to 2018. The NSA just revealed that it had destroyed all the call detail records it had collected since 2015, which would be all those collected under USA Freedom Act.

> Consistent with NSA's core values of respect for the law, accountability, integrity, and transparency we are making public notice that on May 23, 2018, NSA began deleting all call detail records (CDRs) acquired since 2015 under Title V of the Foreign Intelligence Surveillance Act (FISA)
>
> The Government relies on Title V of FISA to obtain CDRs, which do not include the content of any calls. In accordance with this law, the Government obtains these CDRs, following a specific court-authorized process.
>
> NSA is deleting the CDRs because several months ago NSA analysts noted technical irregularities in some data received from telecommunications service providers. These irregularities also resulted in the production to NSA of some CDRs that NSA was not authorized to receive. Because it was infeasible to identify and isolate properly produced data, NSA concluded that it should not use any of the CDRs. Consequently, NSA, in consultation with the Department of Justice and the Office of the Director of National Intelligence, decided that the appropriate course of action was to delete all CDRs. NSA notified the Congressional Oversight Committees, the Privacy and Civil Liberties Oversight

> Board, and the Department of Justice of this decision. The Department of Justice, in turn, notified the Foreign Intelligence Surveillance Court. The root cause of the problem has since been addressed for future CDR acquisitions, and NSA has reviewed and revalidated its intelligence reporting to ensure that the reports were based on properly received CDRs.

Now it could well be these CDRs that NSA was not authorized to collect were selectors that went beyond what had been approved (though that'd be unlikely to trigger a technical alert). It may be these CDRs obtain something that counts as content — such as cookie information that identifies sublevel domains of a webpage.

But the only non content thing that is affirmatively permitted in USAF is location data, which as of last week would get treated as a search if not content. Which leads me to believe this is most likely location data (which would also explain the sudden transparency). It may be content data collected in ways the NSA didn't understand, perhaps via apps that retain the location data shared from the phone. But it's likely it was content data.

And given the specific reference to data "that NSA was not authorized to receive," and the fact that NSA destroyed three years of CDRs, I suspect this, too, was deemed a violation of 1809(a)(2).

Which means the NSA's streak of violating FISA just got extended several more years. It has been violating FISA, in one way or another, for 14 years.