AN ILLEGAL PROGRAM SANCTIONED WITH A RUBBER STAMP IS STILL THAT SAME ILLEGAL PROGRAM

Consider this anecdote from Barton Gellman's story on the many violations of the NSA's spying programs.

> In one instance, the NSA decided that it need not report the unintended surveillance of Americans. A notable example in 2008 was the interception of a "large number" of calls placed from Washington when a programming error confused the U.S. area code 202 for 20, the international dialing code for Egypt, according to a "quality assurance" review that was not distributed to the NSA's oversight staff.
>
> [snip]
>
> In the case of the collection effort that confused calls placed from Washington with those placed from Egypt, it is unclear what the NSA meant by a "large number" of intercepted calls. A spokesman declined to discuss the matter.
>
> The NSA has different reporting requirements for each branch of government and each of its legal authorities. The "202" collection was deemed irrelevant to any of them. "The issue pertained to Metadata ONLY so there were no defects to report," according to the author of the secret memo from March 2013.

Viewed against the background of the documents on the 2009 Section 215 dragnet problems, the anecdote tells us several things:

- The phone metadata for Egypt and for DC were both accessible from the same user interface until at least 2008
- US phone metadata was accessible by area code, not just by single phone identifier
- Because it internally reported this incident, NSA was well aware of that fact
- Among all the violations reported to Reggie Walton in 2009 (see my rough summary), it did not include this one (indeed, it appears NSA has never reported it to FISC, which may be why in response to this story Walton went on the record to complain that the FISA Court relies on the NSA's self-disclosure)

That is, this violation undermines many of the stories the NSA told Walton during the 10 month period when they were purportedly coming clean on major problems with the dragnet, starting with the claim that these problems were a surprise not identified until after he wrote the first substantive opinion — 31 months after FISC first gave it sanction — authorizing the program. (I consider the 2006 opinion authorizing the dragnet a shockingly thin document, and Walton seems to have felt the need to lay out a more substantive case for the legality of it in 2008.)

But something else undermined that story: the pretense that the entire program arose from virgin birth in 2006.

Indeed, we know (though the government hasn't actually admitted it, even though Ron Wyden has asked them to) that the Section 215 dragnet is actually just a part of the Dick Cheney's illegal surveillance program placed under court sanction. Here's how the NSA's own draft IG Report (which was completed right smack dab in the middle of the discussions between Walton and the NSA about these violations) describes some aspects of the program, including the alert program that was part of the initial "discovery" of the violations.

> (TS//SII/OC/NF) Analysis. NSA used a variety of tools to conduct metadata analysis and view the results. NSA's primary tool for conducting metadata analysis, for PSP and traditional SIGINT collection, was MAINWAY. MAINWAY was used for storage, contact chaining, and for analyzing large volumes of global communications metadata. At the beginning of the PSP, only the "SIGINT Navigator" tool was available to view MAINWAY output. Over time, new tools and new processes, such as automated chaining alerting, were created to improve analysts' efficiency. To obtain the most complete results, analysts used data collected under PSP and non-PSP authorities. Typically, they analyzed networks with two degrees of separation (two hops) from the target. Analysts determined if resulting information was reportable.
>
> (TS//SII/OC/NF) In addition, an automated chaining alert process was created to alert analysts of new potentially reportable selectors. Previously approved selectors were compared to incoming MAINWAY data authorized by the PSP, E.O. 12333, or

> the FISC. Alerts of direct contacts with approved selectors were reported to NSA analysts for further analysis and potential reporting to FBI and CIA.

And here's where the IG Report admits this all became the Section 215 dragnet.

> (TS//SV/NF) According to NSA General Counsel Vito Potenza, the decision to transition telephony metadata to the Business Records Order was driven by a private sector company. After the New York Times article was published in December 2005, Mr. Potenza stated that one of the PSP providers expressed concern about providing telephony metadata to NSA under Presidential Authority without being compelled. Although OLC's May 2004 opinion states that NSA collection of telephony metadata as business records under the Authorization was legally supportable, the provider preferred to be compelled to do so by a court order. 11
>
> (TS//SII/NF) As with the PR/TT Order, DoJ and NSA collaboratively designed the application, prepared declarations, and responded to questions from court advisers. Their previous experience in drafting the PR/TT Order made this process more efficient.
>
> (TS//SI//NF) The FISC signed the first Business Records Order on 24 May 2006. The order essentially gave NSA the same authority to collect bulk telephony metadata from business records that it had under the PSP. And, unlike the PRTT, there was no break in collection at transition. The order did, however, limit the number of people that could access the data and required more stringent oversight by and reporting to DOJ. The FISC continues to renew the Business Records Order every 90 days or

> so

And here's where the End-to-End Report the NSA did (this report was completed within a month of the IG Report) admits that one of the violations — the ease with which other Agencies access this data — derived from practices set up under the illegal program.

> NSA learned of CIA, FBI, and NCTC analyst access to unminimized BR FISA metadata-derived query results and target knowledge information via an NSA counterterrorism database. This matter, just recently identified, was a collaboration practice that was in place prior to the inception of the BR FISA Court Order, Over time, approximately 200 analysts at CIA, FBI, and NCTC had been granted access to this target knowledge base. When the BR program was brought under the jurisdiction of the FISA. Court, this practice was not modified to conform with the Order's requirements for the dissemination of BR FISA metadata-derived query results outside of NSA. (16)

The report also admits that another feature of the program, the "Defeat List," dates to 2004.

But perhaps the most troubling passage — and the one that should eliminate any doubts that at least those who had worked on Cheney's illegal program weren't surprised in the least about these "violations" — shows that 19 tools tied to the dragnet were designed to work with the other systems. 7 of those were kluged together (presumably as part of the illegal program) by NSA's Counterterrorism group, not NSA's normal coding people.

> Not designed to be free-standing but the counterpart to the foreign program
>
> These tools and processes, which were designed to function against both the BR

> FISA metadata and other categories of telephony metadata. that NSA acquires through SIGINT operations authorized under the general provisions of EO 12333, were used primarily by analysts within NSA's Office of Counterterrorism to identify possible terrorist connections into, from, and within the U.S., as well as foreign-to-foreign communications. Twelve of the 19 analytic tools examined were developed under [redacted] systems architecture and are well-documented, configuration-controlled and audited. The other seven BR FISA analytic tools examined were developed in whole or in part by engineers working in the Counterterrorism Organization to meet constantly changing mission requirements, resulting in limited configuration and change management control,
>
> [snip]
>
> To mitigate risk in future, NSA will transition the BR FISA analytic tools and processes to the corporate NSA enterprise architecture and will no longer develop tools within the Office of Counterterrorism.
>
> (24-25)

This program was sold (at least in the Intelligence Community's public claims) as a free-standing way to identify US phone users who might have contact with suspected terrorists. But instead, it is clear, it remains the integrated program that ties directly into both international collections (thus the possibility an analyst could pull up DC's phone records when seeking Egypt's) but also content collection. Walton's fixes have eliminated some, but not all, of this integration.

Indeed, one of the other admissions the NSA made

– but not one it offered to fix – in its End-to-End Review is that the protections for this database don't match those promised in the original order.

> In addition, the Court Orders prior to 2 March 2009 state that any processing by technical personnel of the BR metadata acquired pursuant to this Order shall be conducted through the NSA's private network, which shall be accessible only via select machines and only to cleared technical personnel, using secured encrypted communications." The end-to-end review revealed. that the way in which NSA protects the data is not precisely as stated in the Court Order; however we 'believe NSA's implementation is consistent with the intent of preventing unauthorized users from accessing the data. For example, there are not specifically designated or "select" machines from which technical personnel access and process the data on NSA's private, secure network, The internal NSA communications paths on its classified networks are not encrypted, but are subject to strong physical and security access controls which provide the necessary protections.

And once the the continuity between these programs becomes clear, it demonstrates that some claims in the IG Report were almost certainly false.

> (TS//SI//NF) Storage. NSA stored metadata obtained under PSP authorities in a protected database. Only cleared and trained analysts were given access to PSP metadata.
>
> [snip]
>
> NSA did not seek assistance from local exchange carriers, because that would have given NSA access primarily to

> domestic calls.

And some of the comments in the IG Report should raise alarms about even the claims made to Walton during 2009.

> (TS//SI//NF) Regardless of which organization submitted requests or leads to NSA, all resulting reports were sent to CIA and FBI. Reports answered specific RFI questions or provided new investigative leads developed from chaining analysis. Reports contained selectors of interest (potential leads) with potential terrorist connections, not full chaining results: **NSA had minimal insight into how CIA and FBI used PSP products**. [my emphasis]

I'm not yet certain why NSA decided to start "discovering" these violations in 2008. I originally thought it must be the election, but now I wonder whether, after the FISA Amendments Act mandated an IG Report, they realized would have to come clean eventually on these practices.

But it seems very clear that what got reported to Judge Walton as "violations" were in fact the intentional design of the program as it was implemented under the illegal program. They just decided not to fix any of this when they transitioned to the court sanctioned collection program.