ICREACH AND THE 2009 PHONE VIOLATIONS

The Intercept has an article on ICREACH, the middleware NSA implemented between 2005 and 2007 to permit greater sharing of metadata with its IC partners. The article makes this claim.

> ICREACH does not appear to have a direct relationship to the large NSA database, previously reported by *The Guardian*, that stores information on millions of ordinary Americans' phone calls under Section 215 of the Patriot Act. Unlike the 215 database, which is accessible to a small number of NSA employees and can be searched only in terrorism-related investigations, ICREACH grants access to a vast pool of data that can be mined by analysts from across the intelligence community for "foreign intelligence"—a vague term that is far broader than counterterrorism.

I'm fairly certain that is inaccurate.

As I reported on February 6 (at a time when I technically had been hired by the Intercept but not to "report" for them), the circa January 4, 2008 phone dragnet primary order for the first time revealed that the 215 data had been combined with other data "for the purposes of analytical efficiency."

> The Court understands that for the purposes of analytical efficiency a copy of meta data obtained pursuant to the Court's Orders in this matter will be stored in the same database with data obtained pursuant to other NSA authorities and data provided to NSA from other sources. Access to such records shall be strictly limited in accordance with the procedures set forth in paragraphs A – G.

This happened just after ICREACH got generally rolled out in late 2007.

Given the violations "discovered" in 2009, given that NSA used federated queries with Section 215 and PRTT Internet dragnet data at least as late as 2012, I'm fairly certain that the 215 (and PRTT) repositories were made accessible to a more general interface via ICREACH (which one of the documents describes as middleware) at that point. As I've been explaining patiently for over 6 months, the Section 215 phone dragnet we've been arguing about is just one small part of the more general dragnet.

That doesn't mean FBI and DEA and CIA had access to the raw Section 215 metadata (though it ought to raise questions, especially with regards to the Internet dragnet data, for reasons I'll return to). As far as we know, those agencies only got direct access to FISC-authorized phone and Internet dragnet query results, not raw data.

The documents released by the Intercept make it clear other Agencies' analysts would need PKI to log into ICREACH. And that's how — at least after the 2009 phone violations — NSA restricted phone dragnet access to limited numbers of analysts (even while John Bates made the PRTT Internet dragnet data accessible to just about all NSA analysts in 2010). In other words, what the interface did (again, after the 2009 violations anyway) was to ensure that only those with PKI permitting access to the FISC-authorized data could get in and — this was another addition added in 2009 — could only conduct queries using identifiers approved under the more narrow permissions tied to the FISC data. But those NSA analysts who qualified definitely had access to both FISC-authorized and EO 12333 authorized data from the same one-step shop, and for at least a year the FISC-authorized dragnets got subjected to the automatic processes implemented for EO 12333. That was the problem (or one major source of the problem): FISC-authorized phone and Internet

data was being exposed to the processes permitted with EO 12333 data but not permitted with FISC data.

If I'm correct, the inclusion of FISC-approved data in ICREACH led to (or exacerbated) FISC-approved data being treated as EO 12333 data for at least a year. That is, it led to the violations that included (among other things) 3,000 US persons being watchlisted without First Amendment review.

I will have more about what the Intercept documents show later (as well as some thoughts on what the structure of ICREACH might suggest about the NSA's technical problems with the phone dragnet). They answer a number of questions about the metadata dragnet I've been posing for months.

Update: Adding that the point of this sharing is two-way. Not only does NSA share huge amounts of metadata with FBI and CIA, but NSA can contact chain its own metadata with non-metadata from the other agencies (documents mention things like passenger data and clandestine collection). That is, while I don't think FBI and CIA had access to raw BR FISA data (at least not after 2009), I do think NSA was chaining on more than BR FISA.