FEDERATED QUERIES AND EO 12333 FISC WORKAROUND

Particularly given the evidence NSA started expanding its dragnet collection overseas as soon as the FISA Court discovered it had been breaking the law for years, I've been focusing closely on the relationship between the FISA Court-authorized dragnets (which NSA calls BR FISA — Business Records FISA — and PR/TT — Pen Register/Trap and Trace — after the authorities used to collect the data) and those authorized under Executive Order 12333.

This document — Module 4 of a training program storyboard that dates to late 2011 — provides some insight of how NSA trained its analysts to use international collections to be able to share data otherwise restricted by FISC.

The module lays out who has access to what data, then describes how analysts look up both the Reasonable Articulable Suspicion (RAS) determinations of identifiers they want to query on, as well as the BR and PR/TT credentials of those they might share query results with. It also describes how "EAR" prevents an analyst from querying BR or PR/TT data with any non-RAS approved identifier. So a chunk of the module shows how software checks should help to ensure the US-collected data is treated according to the controls imposed by FISC.

But the module also describes how a software interface (almost certainly MARINA, the metadata database) manages all the metadata collected from all over the world.

All of it, in one database.

So if you do what's called a "federated" query with full BR and/or PR/TT credentials — meaning it searches on all collections the analyst has credentials for, with BR and PR/TT being the most restrictive — you may pull metadata

collected via a range of different programs. Alternately, you can choose just to search some of the collections.

> When launching analysts with [redacted] the appropriate BR or PR/TT credentials have the option to check a box if they wish to include BR or PR/TT metadata in their queries. If an analyst checks the "FISABR Mode" or "PENREGISTRY Mode" box when logging into [redacted] will perform a federated query. This means that in addition to either BR or PR/TT metadata, [redacted] will also query data collected under additional collection authorities, depending on the analyst's credentials. Therefore, when performing a query of the BR or PR/TT metadata, analysts will potentially receive results from all of the above collection sources. Users of more recent versions of [redacted] do have the option, however, to "unfederate" the query, and pick and choose amongst the collection sources that they would like to query (10)

Back in 2009, when NSA was still working through disclosures of dragnet problems to FISC, analysts apparently had to guess where the data they were querying came from (which of course is an implicit admission that BR data had been improperly treated with weaker EO 12333 protections for years). But by 2011 they had worked it out so queries showed both what SIGAD (collection point) the metadata came from, as well as (using a classification mark) its highest classification.

> It is possible to determine the collection source or sources of each result within the chain by examining the Producer Designator Digraph (PDDG)/SIGINT Activity Designator (SIGAD) and collection source(s) at the end of the line.

> If at least one source of a result is BR or PR/TT metadata, the classification at the beginning of the line will contain the phrases FISABR or PR/TT, respectively. In addition, in the source information at the end of the line, the SIGAD [redacted] BR data can be recognized by SIGADs beginning with [redacted] For PR/TT, data collected after October 2010 is found [redacted] For a comprehensive listing of all the BR and PR/TT SIGADs as well as information on PR/TT data collected prior to November of 2009, contact your organization's management or subject matter expert.
>
> Since it is possible that one communication event will be collected under multiple collection authorities (and multiple collection sources), not all of the results will be unique to one collection authority (or collection source). Keep in mind that the classification at the beginning of each result only indicates the highest level classification of that result, and does not necessarily reflect whether a result was unique to one collection authority (or collection source). If a result was obtained under multiple authorities (or sources), you will see more [redacted] (15-16)

In other words, analysts will be able to see from their results where the results come from. If a query result includes data only from BR or PR/TT sources, then the analyst can't share the result with anyone not cleared into those programs without jumping some hoops. But if a query result showed other means to come up with the same results from a BR or PR/TT search (that is, if EO 12333 data would return the same result), then the result would not be considered a BR- or PR/TT-unique result, meaning the result could be shared far more widely. (Note, this

passage also provides more details about the timing of the Internet metadata shutdown, suggesting it may have lasted from November 2009 to October 2010.)

> Sharing restrictions in the FISC Orders only apply to unique BR or PR/TT query results. If query results are derived from multiple sources and are not unique to BR and PR/TT alone, the rules governing the other collection authority would apply. (17)

After noting this, the training storyboard spends 5 pages describing the restrictions on dissemination or further data analysis of BR and PR/TT results, even summaries of those results.

Then it returns to the point that such restrictions only hold for BR- or PR/TT-unique results and encourages analysts to run queries under EO 12333 so as to be able to get a result that can be shared and further exploited.

> However, as we've discussed, not all BR or PR/TT results are unique. If a query result indicates it was derived from another collection source in addition to BR or PR/TT, the rules governing the other collection authority would apply to the handling an d sharing of that query result. For example, this result came from both BR and E.O. 12333 collection; therefore, because it is not unique to BR information, it would be ok to inform non- BR cleared individuals of the fact of this communication, as well as task, query, and report this information according to standard E.O. 12333 guidelines.
>
> In summary, if a query result has multiple collection authorities, analysts should source and/or report the non-BR or PR/TT version of that query result according to the rules governing the other authority. But if it is unique

> to either the BR or PR/TT authority then it is a unique query result with all of the applicable BR and PR/TT restrictions placed on it. In both cases, however, analysts should not share the actual chain containing BR or PR/TT results with analysts who do not have the credentials to receive or view BR or PR/TT information. In such an instance, if it is necessary to share the chain, analysts should re-run the query in the non-BR or non-PR/TT areas of [redacted] and share that .cml. (22)

Let me be clear: none of this appears to be illegal (except insofar as it involves a recognition it is collecting US person data overseas, which may raise issues under a number of statutes). It's just a kluge designed to use the US-based dragnet programs to pinpoint results, then use EO 12333 results to disseminate widely.

It does, obviously, raise big questions about whether the numbers reported to Congress on dragnet searches reflect the real number of searches and/or results, which will get more pressing if new information sharing laws get passed.

Mostly, though, it shows how NSA uses overseas collection to collect the same data on Americans without the restrictions on sharing it.

There are a lot of likely reasons to explain why the NSA stopped collecting Internet metadata in the US in 2011 (seemingly weeks after this version of the storyboard, ~~though they would still be able to access the PR/TT metadata for 5 years~~ Update 11/20/14: they destroyed the PRTT data in December 2011). But it is clear the overseas collection serves, in part, to get around FISC restrictions on dissemination and further analysis.

Updated: Added explanation for BR FISA and PR/TT abbreviations.