SOME THOUGHTS ON USA F-REDUX

There's a funny line in the House Judiciary Committee's report on USA F-ReDux. Amid the discussion of the new Call Detail Record function, it explains the government will be doing CDR chaining on "metadata it already lawfully possesses," even as providers will be chaining on metadata in *their* possession.

> In addition, the government can use the FISC-approved specific selection term to identify CDRs from metadata it already lawfully possesses.

The line should not be surprising. As I reported in 2013, the NSA does what are called "federated" queries, metadata chaining across data collected from a variety of sources. This line, then, simply acknowledges that the government will continue to conduct what amounts to federated queries even under the new system.

But the line ought to raise the question, "where does this lawfully possessed data come from?"

The data almost certainly comes from at least 3 sources: metadata taken from PRISM collection in databases that get copied wholesale (so Internet metadata within a hop of a foreign target), records of international phone calls, and records from Internet data collected overseas.

The latter two, of course, would be collected in bulk.

So within the report on a bill many claim ends bulk collection of American's phone records is tacit admission that the bulk collection continues (not to mention that the government has broad access to data collected under PRISM).

After yesterday's 338 – 88 vote in the House in favor of USA F-ReDux, a number of people asked me to explain my view on the bill.

First, the good news. As I noted, while the language on CDR chaining in the actual bill is muddled, the House report includes language that would prohibit most of the egregious provider-based chaining I can imagine. So long as nothing counters that, one of my big concerns dating back to last year has been addressed.

I also opposed USAF last fall because I expected the Second Circuit would weigh in in a way that was far more constructive than that bill, and I didn't want a crappy bill to moot the Second Circuit. While there are many things that might yet negate the Second Circuit ruling (such as conflicting decisions from the DC or 9th Circuits or a reversal by SCOTUS), the Second Circuit's decision was even more useful than I imagined.

But that's part of why I'm particularly unhappy that Specific Selection Term has not been changed to require the government to more narrowly target its searches. Indeed, I think the bill report's language on this is particularly flaccid.

> Section 501(b)(2)(A) of FISA will continue to require the government to make ''a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation….''50 Section 103 requires the government to make an additional showing, beyond relevance, of a specific selection term as the basis for the production of the tangible things sought, thus ensuring that the government cannot collect tangible things based on the assertion that the requested collection''is thus relevant, because the success of [an] investigative tool depends on bulk collection.'' 51 Congress' decision to leave in place the ''relevance'' standard for Section 501 orders should not be construed as Congress' intent to

> ratify the FISA Court's interpretation of that term. These changes restore meaningful limits to the''relevance'' requirement of Section 501, consistent with the opinion of the U.S. Court of Appeals for the Second Circuit in ACLU v.Clapper.

Meaningful limits on "relevant to" would be specific guidelines for the court on what is reasonable and what is not. Instead, USA F-ReDux still subjects the narrowness of an SST to a "greatest extent reasonably practicable" standard, which in the past we've seen amount to prioritization of the practicability of spying over privacy interests. While people can respectfully disagree on this front, I believe USA F-ReDux still permits both bulk collection of non-communications records and bulky collection of communications records (including FBI's Internet collection). In the wake of the Second Circuit opinion, I find that especially inexcusable.

I also am not convinced USA F-ReDux is an across-the-board privacy win. I argued last year that USAF swaps a well-guarded unexploded nuclear bomb for many more exploding IEDs striking at privacy. By that, I mean that the new CDR function will probably not result in any less privacy impact, in practice (that is, assuming NSA follows its own minimization rules, which it hasn't always), than the prior dragnet. That's true because:

- We have every reason to believe the CDR function covers all "calls," whether telephony or Internet, unlike the existing dragnet. Thus, for better and worse, far more people will be exposed to chaining than under the existing dragnet.

It will catch more potential terrorists, but also more innocent people. As a result, far more people will be sucked into the NSA's maw, indefinitely, for exploitation under all its analytical functions. This raises the chances that an innocent person will get targeted as a false positive.

- The data collected under the new CDR function will be circulated far more broadly than status quo. Existing dragnet orders limit access to the results of queries to those with special training unless one of four named individuals certifies that the query result relates to counterterrorism. But USA F-ReDux (and the current minimization procedures for Section 702 data; USA F-ReDux will likely use the PRISM infrastructure and processing) makes it clear that FBI will get access to raw query results. That almost certainly means the data will be dumped in with FBI's PRISM and FISA data and subjected to back door searches at even the assessment level, even for

> investigations that have nothing to do with terrorism. As on the NSA side, this increases the risk that someone will have their lives turned upside down for what amounts to being a false positive. It also increases the number of people who, because of something in their metadata that has nothing to do with a crime, can be coerced into becoming an informant. And, of course, they'll still never get notice that that's where this all came from, so they will have a difficult time suing for recourse.

One other significant concern I've got about the existing bill — which I also had last year — is that the emergency provision serves as a loophole for Section 215 collection; if the FISC deems emergency collections illegal, the government still gets to keep — and parallel construct — the data. I find this especially concerning given how much Internet data FBI collects using this authority.

I have — as I had last year — mixed feelings about the "improvements" in it. I believe the amicus, like initial efforts to establish PCLOB, will create an initially ineffective function that might, after about 9 years, someday become effective. I believe the government will dodge the most important FISC opinion reporting, as they currently do on FOIAs. And, in spite of a real effort from those who negotiated the transparency provisions, I believe that the resulting reporting will result in so thoroughly an affirmatively misleading picture of

surveillance it may well be counterproductive, especially in light of the widespread agreement the back doors searches of Section 702 data must be closed (while there are a few improvements on reporting *to Congress* in this year's bill, the public reporting is even further gutted than it was last year).

And now there's new gunk added in.

One change no one has really examined is a change extending "foreign power" status from those proliferating WMDs to those "conspiring" or "abetting" efforts to do so. I already have reasons to believe the WMD spying under (for example) PRISM is among the more constitutionally problematic. And this extends that in a way no one really understands.

Even more troublesome is the extension of Material Support maximum sentences from 15 to 20 years. Remember, under Holder v. HLP, a person can be convicted of material support for First Amendment protected activities. Thus, USA F-ReDux effectively embraces a 20 year sentence for what could be (though isn't always) thought crimes. And no one has explained why it is necessary! I suspect this is an effort to use harsh sentences to coerce people to turn informant. If so, then this is an effort to recruit fodder for infiltrators into ISIS. But if all that's correct, it parallels similar efforts under the Drug War to use excessive sentences to recruit informants, who — it turns out in practice — often lead to false convictions and more corruption. In other words, at a moment when there is bipartisan support for sentencing reform for non-violent crimes (for which many cases of Material Support qualify), USA F-ReDux goes in the opposite direction for terrorism, all at a time when the government claims it should be putting more emphasis on countering extremism, including diversion.

So while I see some advantages to the new regime under USA F-ReDux (ironically, one of the most important is that what surveillance the government does will be less ineffective!), I am

not willing to support a bill that has so many bad things in it, even setting aside the unconstitutional surveillance it doesn't address and refuses to count in transparency provisions. I think there need to be privacy advocates who live to fight another day (and with both ACLU and EFF withdrawing their affirmative support for the bill, we at least have litigators who can sue if and when we find the government violating the law under this new scheme — I can already identify an area of the bill that is certainly illegal).

That said, it passed with big numbers yesterday. If it passes, it passes, and a bunch of authoritarians will strut their purported support for liberty.

At this point, however, the priority needs to be on preventing the bill from getting worse (especially since a lot of bill boosters seem not to have considered at what point they would withdraw their support because the bill had gotten too corrupted). Similarly, while I'm glad bill sponsors Jim Sensenbrenner and Jerry Nadler say they won't support any short-term extension, that may tie their own hands if what comes back is far worse than status quo.

There's some good news there, too. The no votes on yesterday's House vote were almost exclusively from supporters of privacy who believe the bill doesn't go far enough, from Justin Amash to Jared Polis to Tom Massie to Donna Edwards to Ted Poe to rising star Ted Lieu and — most interestingly — Jan Schakowsky (who voted for the crappier House bill when she was on HPSCI last year). Hopefully, if and when Mitch McConnell throws in more turdballs, those who opposed the bill yesterday can whip efforts to defeat it.

Stay tuned.