TEN GOODIES USA F-REDUX GIVES THE INTELLIGENCE COMMUNITY

Update, November 20, 2015: I've updated (and corrected, in the case of the parallel construction loophole) this post here.

Amid renewed tactical leveraging from Mitch McConnell, USA F-ReDux boosters continue to remain silent (or worse, in denial) about the many advantages USA F-ReDux offers the Intelligence Community over the status quo.

But there are many reasons — aside from the general uselessness of the phone dragnet in its existing form — why USA F-ReDux is an improvement for the Intelligence Community. That doesn't mean it doesn't also have benefits for reformers (though we can respectfully disagree about how real those benefits are). It just means it also has at least as many benefits for the IC. Some of these are:

1. Inclusion of Internet calls, along with phone calls, in chaining system

Up until 2009, and then again from 2010 to 2011, NSA had two interlocking systems of domestic metadata tracking: the phone dragnet under Section 215 and the Internet dragnet under PRTT. ~~Since the government shut down the latter, however, it has likely lost access to some purely domestic links that can't be collected (and chained under SPCMA) overseas.~~

Update, May 7: According to Richard Burr, the government has been collecting IP "addresses," so I guess they already include Internet access in their dragnet.

USA F-ReDux is technology neutral; unlike phone

dragnet orders, it does not limit collection to telephony calls. This probably means the government will fill the gap in calls that has been growing of late (which anonymous sources have dubiously claimed to make up 70% of all calls). While it's unlikely the NSA is really missing 70% of all domestic calls of interest, closing a significant gap of any kind will be a huge benefit for the IC.

2. Addition of emergency provision for all Section 215 applications

Currently, there is a FISC-authorized emergency provision for the phone dragnet, but not the rest of Section 215 production. That's a problem, because the most common use of Section 215 is for more targeted (though it is unclear how targeted it really is) Internet production, and the application process for Section 215 can be slow. USA F-ReDux makes emergency application procedures available for all kinds of Section 215 applications.

3. Creation of giant parallel construction loophole under emergency provision

Not only does USA F-ReDux extend emergency provision authority to all Section 215 applications, but it changes the status quo FISC created in a way that invites abuse. That's because, even if the FISC finds an agency collected records improperly under the emergency provision, the government doesn't have to destroy those records. Indeed, the only restriction on those records is that they cannot be entered into any official proceeding. The Attorney General polices this, not the FISC. ~~Moreover, the bill says nothing about derivative records.~~ This is tantamount to saying that the government can do whatever it wants using the emergency provisions, so long as it promises to

parallel construct improperly collected records if they want to use them against an American. The risk that the government will do this is not illusory; in the year since FISC created this emergency provision, they've already had reason to explicitly remind the government that even under emergency collection, the government still can't collect on Americans solely for First Amendment protected activities.

4. Provision for a super-hop that might be used to access unavailable smart phone data

As happened last year, no one seems to understand the chaining procedure that is the heart of this bill. What's clear is that, as written, it does not do what every news article (save mine) say it does; it does not simply provide an extra "hop" of call data. The language appears to permit the government to ask providers to use session-identifying information that cannot be collected (which might include things like location or super-cookies) to provide additional data that does fit the definition of Call Detail Record. As an example, the government might be able to ask providers to use location data to find co-located phones, which is a service AT&T already offers under Hemisphere; the government would only get the device identifiers for the phones, not the location itself, but would benefit from that location data. Another possible application would be to ask providers to use supercookie data to track online behavior. While there are likely good reasons for permitting the government to ask providers to conduct analysis on non CDR session identifying information — such as it provides a way for providers to help the government find burner phones or accounts — without more oversight or limiting language it might be very badly abused.

5. Elimination of pushback from providers

USA F-ReDux gives providers two things they don't get under existing Section 215: immunity and compensation. This will make it far less likely that providers will push back against even unreasonable requests. Given the big parallel construction loophole in the emergency provisions and the super-hop in the chaining provision, this is particularly worrisome.

6. Expansion of data sharing

Currently, chaining data obtained under the phone dragnet is fairly closely held. Only specially trained analysts at NSA may access the data returned from phone dragnet queries, and analysts must get a named manager to certify that the data is for a counterterrorism purpose to share outside that group of trained analysts. Under this bill, all the returned data will be shared — in full, apparently — with the NSA, CIA, and FBI. And while the bill would require the government to report how often NSA and CIA does back door searches of the data, the FBI would be exempted from that reporting requirement.

Thus, this data, which would ostensibly be collected for a counterterrorism purpose, will apparently be available to FBI every time it does an assessment or opens up certain kinds of intelligence, even for non-counterterrorism purposes. Furthermore, because FBI's data sharing rules are much more permissive than NSA's, this data will be able to be shared more widely outside the federal government, including to localities. Thus, not only will it draw from far more data, but it will also share the data it obtains far more broadly.

7. Mooting of court

challenges

Passage of USA F-ReDux would also likely moot at least the challenges to the phone dragnet (there are cases before the 2nd, 9th, and DC Circuits right now, as well as a slightly different challenge from EFF in Northern California). That's important because these challenges — particularly as argued in the 2nd Circuit — might get to the underlying "relevant to" decision issued by the FISC back in 2004, as well as the abuse of the 3rd party doctrine that both bulk and bulky collection rely on. That's important because USA F-ReDux not only does nothing about that "relevant to" decision, it relies on the language anew in the new chaining provision.

The bill would probably also moot a challenge to National Security Letter gag orders EFF has.

Update, May 7. Oops! I guess Congress didn't move quickly enough to moot the 2nd Circuit.

8. Addition of 72-hour spying provisions

In addition to the additional things the IC gets related to its Section 215 spying, there are three unrelated things the House added. First, the bill authorizes the "emergency roamer" authority the IC has been asking for since 2013. It permits the government to continue spying on a legitimate non-US target if he enters the US for a 72-hour period, with Attorney General authorization. While in practice, the IC often misses these roamers until after this window, this will save the IC a lot of paperwork and bring down their violation numbers.

9. Expansion of proliferation-related spying

USA F-ReDux also expands the definition of "foreign power" under FISA to include not just

those proliferating in weapons of mass destruction, but also those who “knowingly aid or abet” or “conspire” with those doing so. This will make it easier for the government to spy on more Iran-related targets (and similar such targets) in the US.

10. Lengthening of Material Support punishments

In perhaps the most gratuitous change, USA F-ReDux lengthens the potential sentence for someone convicted of material support for terrorism — which, remember, may be no more than speech! — from 15 years to 20. I’m aware of no real need to do this (except, perhaps, to more easily coerce people to inform for the government). But it is clearly something someone in the IC wanted.

Let me be clear: some of these provisions (like permission to chain on Internet calls) will likely make the chaining function more useful and therefore more likely to prevent attacks, even if it will also expose more innocent people to expanded spying. Some of these provisions (like the roamer provision) are fairly reasonably written. Some (like the changes from status quo in the emergency provision) are hard to understand as anything but clear intent to break the law, particularly given IC intransigence about fixing obvious problems with the provision as written. I’m not claiming that all of these provisions are bad for civil liberties (though a number are very bad).

But to pretend these don’t exist — to pretend the IC isn’t getting a whole lot that it has been asking for, sometimes for as long as 6 years — is either bad faith or evidence of ignorance about what the existing dragnet does and what this bill would do. It’s also bad negotiating strategy.