10 GOODIES USA FREEDOM ACT GIVES THE INTELLIGENCE COMMUNITY

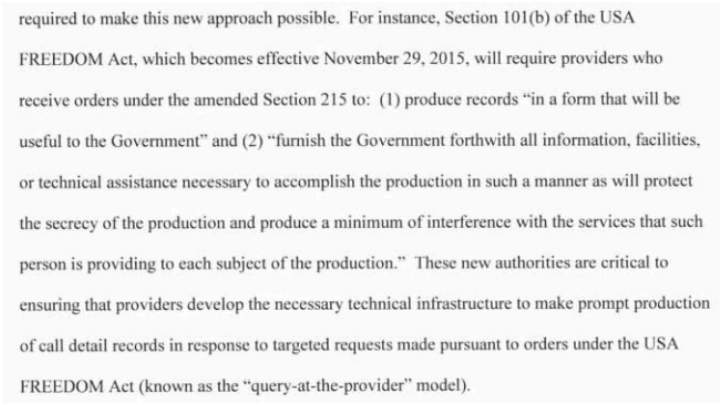
Since the Paris attack has turned much of our country into a shriveling pack of cowards, Republicans have ratcheted up claims that USA Freedom Act will make us less safe. Those claims tend to be so ignorant they claim the law — passed in June but not fully implemented until a week from Sunday — prevented the Intelligence Community from preventing the Paris attack. That would not be possible for two reasons. First, because the key provision hasn't started yet (though some of the benefits for the IC have). And, because according to reports the network that carried out the Paris attack had no ties to the US, and therefore the dragnet couldn't have shown anything useful.

All that said, I thought both the fear-mongering and the imminent changeover made it a good time to update (and in a few places, correct) this post, which laid out 10 things the IC gets out of USAF.

1. Inclusion of cell and (probably) some Internet "calls" in chaining system

Since early 2014, intelligence sources have been leaking that the phone dragnet misses 70% of US calls. That number is probably an exaggeration (and doesn't account for what the NSA collects under significantly redundant collection under EO 12333). But there are probably several reasons for why the old dragnet had incomplete coverage. First, providers that only keep cell records with location data attached could not be obligated to turn over those records under the existing program (when AT&T started turning over cell records in 2011, it stripped location data

for the NSA voluntarily, but no providers were obligated to do so). In a declaration submitted in Larry Klayman's challenge to the phone dragnet, NSA makes it clear the ability to demand production in the form NSA wants is one big difference in the program (as is having facilities onsite, which probably mirrors the PRISM program).



required to make this new approach possible. For instance, Section 101(b) of the USA FREEDOM Act, which becomes effective November 29, 2015, will require providers who receive orders under the amended Section 215 to: (1) produce records "in a form that will be useful to the Government" and (2) "furnish the Government forthwith all information, facilities, or technical assistance necessary to accomplish the production in such a manner as will protect the secrecy of the production and produce a minimum of interference with the services that such person is providing to each subject of the production." These new authorities are critical to ensuring that providers develop the necessary technical infrastructure to make prompt production of call detail records in response to targeted requests made pursuant to orders under the USA FREEDOM Act (known as the "query-at-the-provider" model).

In addition, USA Freedom is technology neutral; unlike phone dragnet orders, it does not limit collection to telephony calls, though it does limit collection to "phone companies," which I presume includes handset makers Apple, Microsoft, and Google. This probably means the government will fill the gap in calls that has been growing of late, probably including VOIP and iMessage.

2. Addition of emergency provision for all Section 215 applications

Before USAF passed, there was a FISC-authorized emergency provision for the phone dragnet, but not the rest of Section 215 production. That was 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. USAF made emergency application procedures available for all kinds of Section 215 applications.

3. Creation of parallel construction loophole under emergency provision

Not only does USAF 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. It prohibits the use of "derivative" evidence in any proceeding, but there is abundant reason to believe the government still finds a way to parallel construct evidence even in other laws with such limitation on "derivative" evidence and so we should expect the same to happen here. The risk that the government will do this is not illusory; in the 18 months or so 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. Chaining on "connections" rather than "calls," which might be used to access unavailable smart phone data

Rather than chaining on calls made, USAF chains on "connections," with Call Detail Record defined based on "session identifier." This is probably intended to permit the government to obtain the call records of "correlated" identities, including things like all the records from a "Friends and Family" account. And while the House Report specifically prohibited some potentially troubling uses (like having providers chain on location information), in the era of smart phones and super cookies, the language of the bill leaves open the possibility

of vastly expanded “connections.”

5. Elimination of pushback from providers

USAF 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 parallel construction loophole in the emergency provisions and the potentially expansive uses of connection chaining, 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 new law, all the returned data will be shared — in full, apparently — with the NSA, CIA, and FBI. And the FBI is exempted from reporting on how many back door searches it does of this data.

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

As we've seen in both ACLU v. Clapper and Klayman v. Obama, USAF mooted court challenges to the dragnet, including ones that looked likely to rule the expansive "relevant to" based collections unconstitutional. In addition, the law may moot EFF's First Unitarian Church v. NSA challenge to the dragnet, which of all the challenges is most likely to get at some of the underlying constitutional problems with the dragnet.

8. Addition of 72-hour spying provisions

In addition to the additional things the IC got related to its Section 215 spying, there are three unrelated things the House added. First, the law authorized 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

USAF also expanded 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, USAF lengthened 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 all of them are (or were, for those that have already gone into force) clear expansions on the authorities and capabilities the IC used to have.