FOUR REASONS USA FREEDUMBER IS WORSE THAN THE STATUS QUO

In the post-HR 3361 passage press conference yesterday, Jerry Nadler suggested the only reason civil libertarians oppose the bill is because it does not go far enough.

That is, at least in my case, false.

While I have concerns about unintended consequences of outsourcing holding the call data to the telecoms (see my skepticism that it ends bulk collection here and my concerns about high volume numbers here), there are a number of ways that USA Freedumber is worse than the status quo.

These are:

- The move to telecoms codifies changes in the chaining process that will almost certainly expand the universe of data being analyzed
- In three ways, the bill permits phone chaining for purposes outside of counterterrorism
- The bill weakens minimization procedures on upstream collection imposed by John Bates, making it easier for the government to collect domestic content domestically
- The bill guts the current controls on Pen Register

> authority, making it likely the government will resume its Internet dragnet

The NSA in your smart phone: Freedumber codifies changes to the chaining process

As I have described, the language in USA Freedumber makes it explicit that the government and its telecom partners can chain on *connections* as well as actual phone call contacts. While the new automatic search process approved by the FISA Court in 2012 included such chaining, by passing this bill Congress endorses this approach. Moreover, the government has never been able to start running such automatic queries; it appears they have to outsource to the telecoms to be able to do so (probably in part to make legal and technical use of location data). Thus, moving the phone chaining to the telecoms expands on the kinds of chaining that will be done with calls.

We don't know all that that entails. At a minimum (and, assuming the standard of proof is rigorous, uncontroversially) the move will allow the government to track burner phones, the new cell phones targets adopt after getting rid of an old one.

It also surely involves location mapping. I say that, in part, because if they weren't going to use location data, they wouldn't have had to move to the telecoms. In addition, AT&T's Hemisphere program uses location data, and it would be unrealistic to assume this program wouldn't include at least all of what Hemisphere already does.

But beyond those two functions, your guess is as good as mine. While the chaining must produce a Call Detail Record at the interim step (which limits how far away from actual phone calls the analysis can get), it is at least conceivable the chaining could include any of a number of kinds of data available to the telecoms from smart phones, including things like calendars,

address books, and email.

The fact that the telecoms and subsidiary contractors get immunity and compensation makes it more likely that this new chaining will be expansive, because natural sources of friction on telecom cooperation will have been removed.

Freedumber provides three ways for NSA to use the phone dragnet for purposes besides counterterrorism

As far as we know, the current dragnet may only be used for actual terrorist targets and Iran. But USA Freedumber would permit the government to use the phone dragnet to collect other data by:

- Requiring only that selection terms be associated with a foreign power
- Permitting the retention of data for foreign intelligence, not just counterterrorism, purposes
- Allowing the use of emergency queries for non-terrorism uses

Freedumber permits searches on selection terms associated with foreign powers

On its face, USA Freedumber preserves this counterterrorism focus, requiring any records obtained to be "relevant to" an international terrorist investigation. Unfortunately, we now know that FISC has already blown up the meaning of "relevant to," making all data effectively relevant.

The judicial approval of the specific selection term, however — the court review that should be an improvement over the status quo — is not that tie to terrorism, but evidence that the selection term is a foreign power or agent

thereof.

Thus, the government could cite narcoterrorism, and use the chaining program to investigate Mexican drug cartels. The government could raise concerns that al Qaeda wants to hack our networks, and use chaining to investigate hackers with foreign ties. The government could allege Venezuela supports terrorism and investigate Venezuelan government sympathizers.

There are a whole range of scenarios in which the government could use this chaining program for purposes other than counterterrorism.

Freedumber permits the retention of any data that serves a foreign intelligence purpose

And once it gets that data, the government can keep it, so long as it claims (to itself, with uncertain oversight from the FISC) that the data has a foreign intelligence purpose.

At one level, this is a distinction without a difference from the language that USA Freedumb had used, which required the NSA to destroy the data after five years unless it was relevant to a terrorism investigation (which all data turned over to NSA would be, by definition). But the change in language serves as legislative approval that the use of the data received via this program can be used for other purposes.

That will likely have an impact on minimization procedures. Currently, the NSA needs a foreign intelligence purpose to access the corporate store, but can only disseminate data from it for counterterrorism purposes. I would imagine the changed language of the bill will lead the government to successfully argue that the minimization procedures permit the dissemination of US person data so long as it meets only this flimsy foreign intelligence purpose. In other words, US person data collected in chaining would be circulating around the government more freely.

Freedumber's emergency queries do not require any tie to terrorism

As I noted, the revisions USA Freedumber made to USA Freedumb explicitly removed a requirement that emergency queries be tied to a terrorism investigation.

> (A) reasonably determines that an emergency situation requires the production of tangible things to ~~obtain information for an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to protect against international terrorism~~ before an order authorizing such production can with due diligence be obtained;

That's particularly troublesome, because even if the FISC rules the emergency claim (certified by the Attorney General) was not legally valid after the fact, not only does the government *not* have to get rid of that data, but the Attorney General (the one who originally authorized its collection) is the one in charge of making sure it doesn't get used in a trial or similar proceeding.

In short, these three changes together permit the government to use the phone dragnet for a lot more uses than they currently can.

Freedumber invites the expansion of upstream collection

When John Bates declared aspects of upstream collection to be unconstitutional in 2011, he used the threat of referrals under 50 USC 1809(a) to require the government to provide additional protection both to entirely domestic communications that contained a specific selector, and to get rid of domestic communications that did not contain that specific selector at all. The government objected (and considered appealing), claiming that because it hadn't really intended to collect this data, it should be able to keep it and use it. But ultimately, that threat (especially threats tied to the government's use

of this data for ongoing FISA orders) led the government to capitulate.

The changes in Freedumber basically allow the government to adopt its old "intentional" claim, reversing Bates' restrictions. That's because they only have to extend protection to domestic communications if they're from an identifiable US person, rather than from a US person location (NSA has claimed they have a hard time identifying a lot of this data). And, more troubling, they only have to minimize such communications if they recognize them as such at the moment they collect it. Finally, they only have to do so "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information," basically providing the government a giant loophole not even to do that.

Effectively, then, this language on upstream searches will permit the government to use upstream searches to collect and keep domestic communications because they need to collect foreign intelligence.

Under Freedumber, the government will almost certainly resume the Internet dragnet

In a very similar but even more alarming fashion, USA Freedumber also reverses John Bates' 2010 efforts to shut down the illegal Internet dragnet.

As I explained in this post, from the very start of the FISC-sanctioned dragnet, the government claimed that the Pen Register statute permitted the judge only a very circumscribed role rubber stamping applications. Effectively, revised language in USA Freedumber would codify that stance in law.

Of particular concern, USA Freedumber replaced USA Freedom Act's language codifying minimization procedures (and FISC's ability to review compliance with them) with language requiring the Attorney General to develop privacy procedures. The application of those procedures, like the minimization procedures for

upstream collection, will be secondary to "the need to protect national security."

In addition, USA Freedumber exempts PRTT from some of the reporting requirements, making the detailed practices of PRTT less visible to Congress.

From what we know about the Internet dragnet, Colleen Kollar-Kotelly imposed limits on the Internet dragnet, which the NSA violated — and lied about — right away. As part of the reviews done in 2009, FISC discovered NSA was still and always had been violating those restrictions. Internet dragnet collection may have been halted from 2009 to 2010, but in 2010, Bates reimposed limits (it's not clear if these were the same ones imposed by Kollar-Kotelly). The NSA "shut down" the program a year or so after Bates imposed those limits (though there are reasons to doubt it got shut down, rather than just moved), apparently because it just wasn't all that useful once they had to follow the rules. Bates used two levers to be able to impose these requirements: the assumption he could impose minimization procedures, and that threat of using 50 USC 1809(a) to limit the use of illegally collected data going forward.

By explicitly denying FISC the authority to impose minimization procedures, USA Freedumber effectively takes away all the leverage FISC used to ensure that the Internet dragnet stopped being domestic content acquisition program.

The only question is whether the requirement that all production begin from a "specific selection term" would prevent the resumption of the Internet dragnet. I don't think it would. That's because the entire program always was based on specific selection terms — tied to telecom circuits, based on the claim those circuits carried a higher percentage of terrorism traffic than other circuits. By resuming the Internet dragnet on those circuits (but not all of them, thereby using a discriminator), NSA can claim it is not engaging in bulk collection, and still get away with

resuming the Internet dragnet.

And the best part? The telecoms would now have immunity to help NSA collect domestic content in the US.

Just before the vote yesterday, the tech companies withdrew their support for the bill, saying that "The latest draft opens up an unacceptable loophole that could enable the bulk collection of Internet users' data." They appear to believe the loophole derives from the wide open definition of "specific selection term." But if I'm right about these last two changes, then the loophole is salted throughout the bill. And it would put the telecoms back in the business of stealing Internet content (to the extent that it is accessible) as it passed their backbone. If I'm right about that — and if the Internet companies realize it — then we have a hope of preventing this shitty, worse than status quo bill from becoming law.

But whether we will nor not remains to be seen.

Update: Given the way I believe US Freedumber guts leverage that John Bates exercised over NSA, I find this comment from him — from 3 weeks ago — striking.

> Bates also sounded dubious about proposals—like Obama's—to have phone companies store call metadata instead of the government. The judge said he's more confident that "compliance" issues can be addressed at a government agency like the NSA than at private companies.
>
> "My experience tells me that I can hold the NSA's feet to the fire a lot easier than I can hold Google or Verizon's feet to the fire," Bates said. He noted that he has considerable leverage over the NSA, because they want to keep running the program and need the court's permission to do so. On the other hand, "the private companies want the program cut off," so would have less incentive to address problems, he added.