



Getting Under the Hood of the HPSCI Bulk Collection Bill

By Julian Sanchez

Monday, March 31, 2014

While details on the president’s proposal to end NSA bulk collection of telephony records [remain sparse](#), we do now have an [actual piece of legislation](#) to look at from the House Permanent Select Committee on Intelligence—one that tracks the broad outlines of the White House plan even as it differs in several critical details. I’ve already done a quick take in broad brushstrokes [over at *The Daily Beast*](#); here I want to get into the weeds a bit.

The HPSCI bill actually covers quite a bit more than just NSA bulk collection—there are a few transparency measures and a provision for the FISA Court to appoint amici curiae, which mostly seems like an attempt to preempt legislation creating a more robust FISC “advocate”—but in this post I want to focus on the meat: The prohibition (or so it seems) on bulk collection, and the new authority in §503 designed to replace the current bulk telephony program.

(A) The Bulk Prohibition

The first thing to note is that the (apparent) prohibition on bulk collection is structured somewhat oddly, even taking into account the framers apparent desire to limit that prohibition to certain subcategories of records. The USA Freedom Act, for instance, does this by means of a fairly straightforward modification: It limits the scope of §215 (as well as FISA pen/trap orders and National Security letters) to records that are both relevant to an investigation *and* pertain to a suspected foreign agent or their direct contacts, using language the Senate had unanimously approved back in 2005. The HPSCI bill is rather bit more convoluted.

First, Section 2 of the bill *completely excludes* “call detail records” from the scope of §215—and *only* from §215. The bill defines “call detail records” as “communications routing information,” which sounds awfully general, but both the description as “call detail records” and the series of enumerated telephony-specific data types that follow [strongly suggest](#) it’s really limited to *telephonic* communications routing information. There’s some wiggle room here since [the general term precedes the more specific enumeration](#), but especially in light of the subsequent

separate prohibition on acquisition of “electronic communications” records, defined to exclude telephonic communications, I’d be surprised if the FISC didn’t read this narrowly. Though the “including” that precedes the enumerated data types indicates that it’s not exhaustive, the omission of location-associated terms like “cell site and sector” is conspicuous. HPSCI staff are apparently assuring reporters that location data is implicitly included, but we do know that law enforcement routinely obtain bulk location data in the form of “[tower dumps](#),” or records of all the phones registered with a specific cell tower at a particular time. Since phones routinely do this even when they’re not placing a call—which is to say, when no particular “communication” is being “routed”—it’s at least an open question whether this provision forbids bulk collection of tower location data.

Then Section 3, “notwithstanding any other provision of law,” prohibits the government from acquiring “records of any electronic communication without the use of specific identifiers or selection terms” under *any* provision of FISA. Contrast the White House proposal, which from what we’ve heard so far would not impose any limits on non-telephony collection. This section incorporates the Electronic Communications Privacy Act definition of “electronic communications,” which as noted above, means it *excludes* records of phone calls or other “aural transfer” (e.g. VoIP), which fall under the mutually exclusive category of “wire communications.” Later in §503, the bill explicitly refers to both “electronic” and “wire” communications records, suggesting that this is very much intentional. This provision, then, would not appear to preclude bulk collection of telephony metadata (“call detail records”) under FISA authorities other than §215. Nor, of course, does it apply to National Security Letters, which are issued by the heads of FBI field offices without judicial pre-approval, since those are not technically part of FISA, despite generally being used in the same investigations.

Also left ambiguous is precisely what “specific identifiers or selection terms” means. Intuitively it would refer to things like e-mail addresses and account logins, but documents leaked by Edward Snowden suggest that in some contexts the government has used much broader “selectors,” such as ranges of Internet Protocol addresses. If something that broad can count as a “specific identifier,” then at the outer limits the distinction between “targeted” and “bulk” collection becomes somewhat semantic.

Finally, note that the prohibition here only applies to the “acquisition” of a “record.” Crucially, collection of information live from the wire pursuant to [50 USC §1842](#), the provision that authorized NSA’s now-defunct bulk Internet metadata program, probably **does not** count as the “acquisition of a record,” even though, intuitively, it is a process by which the government ends up with records of communications. A former intelligence official I informally bounced this language off agreed that the use of this pen register/trap-and-trace provision would not fall under this prohibition, because the information obtained isn’t acquired *in the form of* a record maintained by a communications provider: Rather, the government is acquiring data in transit and *creating* its *own* record rather than “acquiring” one.

The last prohibition, similarly covering all FISA authorities, bars acquisition without specific identifiers of several other categories of sensitive records, specifically:

library circulation records, library patron lists, book sales records, book customer lists, firearm sales records, tax return records, educational records, or medical records containing information that would identify a person

This is the same list of sensitive records currently requiring explicit approval by Attorney General before they can be acquired under §215. The final qualifier—“containing information that would identify a person”—is likely to be read as applying to all the preceding types of information. In addition to the other loopholes and ambiguities, this might be read to allow bulk acquisition of “anonymized” records for various data mining purposes. Anonymization, however, should not obviate privacy concerns: As [Paul Ohm has documented](#), any sufficiently rich and informative “anonymous” data set can be re-identified given enough other data sets—which the NSA has in abundance. And of course, many types of records not specifically named—credit card records, for instance—are not included in any of these prohibitions (or pseudo-prohibitions) on bulk collection.

(B) The New Authority

In order to preserve the capabilities of the current NSA telephony program, the HPSCI bill created a new and distinct authority, §503, that authorizes rapid collection of both telephony and electronic communications metadata under a process superficially somewhat similar to §702 of the FISA Amendments Act. The Attorney General and Director of National Intelligence jointly issue broad “authorizations” for the collection of records pertaining to suspected agents of foreign powers and their direct contacts or associates. (This effectively gives you two “hops” from a “seed” number: The direct contact is the first hop and their records contain identifiers for the second hop.) Records must not include communications content or other personally identifying information, and procedures must be developed to protect privacy and civil liberties. The FISC signs off on general procedures for establishing “reasonable articulable suspicion” of the appropriate foreign power link in the selectors that providers are directed to provide records on. The government then issues directives to telecom providers requiring both historical and prospective, ongoing production of records pertaining to specific identifiers. The FISC does *not* pre-approve these directives and selectors, but must be “promptly” provided with each directive and a record of the basis for thinking it meets the criteria—at which point the court can terminate acquisition if it believes the criteria are not met, though no further *affirmative* approval is required.

While it may not be obvious, probably the critical thing here is actually the provision requiring the providers to produce “records, whether existing or created in the future, in the format specified by the Government” coupled with one providing for the providers to be compensated and receive any necessary technical assistance from the government. For domestic phone numbers, after all, FISA pen register authority already covers this type of collection, and *many* providers should be able to do a historical search of their records for foreign numbers. But the CALEA J-standard spelling out the surveillance capabilities that telecoms are required to have seems to assume that “pen registers” are always and only applied to a specific “facility” corresponding to a customer phone line. The trick, in other words, was rapidly getting the carriers to produce records of calls to or from specific *foreign* numbers—and to produce them in a format that made it easy to cross-reference records across carriers. In other words, this

provision lets the government demand that the carriers *create records in the form they need*, even if the company doesn't maintain records of that type for its own business purposes, with government money and tech support to help them do it.

The HPSCI authority differs from the §215 statute, the current telephony program, and the president's proposal in several salient ways.

The very first words of §503 capture one difference: “notwithstanding any other law.” While ultimately the FISC has apparently not been much deterred by the absence of a “notwithstanding” provision in §215, it does at least in principle mean that §215 does not automatically trump other statutory protections—and as a rule one wants these “notwithstanding” provisions used sparingly in broad collection authorities. Without access to the FISC's other §215 opinions, it is hard to say what effect—if any—this addition will have.

Unlike the current telephony program (and apparently the president's proposal), this authority is not restricted to identifiers tied to any particular terrorist group. Rather, a link (based on reasonable suspicion) to any foreign power or agent of a foreign power will suffice. The “reasonable suspicion” nexus is, obviously, narrower than the requirement of “relevance” required by §215 as currently interpreted by the FISC—and indeed, narrower even than the common pre-Snowden understanding of §215.

What is **entirely eliminated** required link to “an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.” Given the breadth of FBI “enterprise investigations,” frequently invoked by defenders of the FISC's strained “relevance” ruling, one would not think that requirement would prove unduly burdensome in practice. Removing it, however, does a couple things: First, it eliminates whatever check might have been provided by the predication requirements for opening an investigation, and unmoors the acquisition authority from any particular investigative target. In at least *some* cases, this specific investigative link has tipped off the FISC that a record request might run afoul of the proscription on targeting Americans (presumably journalists) based solely on First Amendment protected conduct. If the FISC is *only* evaluating the foreign power link, that warning flag might not go up. Second—and perhaps more importantly—**it would appear to eliminate the requirement that records pertaining to U.S. persons be acquired only for counterterrorism or counterespionage investigations**, rather than for “foreign intelligence purposes” generally, which might include almost any effort to understand the actions and intentions of foreign entities. In practice, of course, these have not been effective limits on the *acquisition* of records, but the FISC *has* at least tried to embody these limits in back-end querying and usage limitations.

The most obvious difference from what the president has proposed—beyond the application to non-telephony communications records—is of course the combination of ex-ante FISC approval of programmatic procedures coupled with ex-post review of specific directives, instead of the pre-approval of specific selector queries that the president has endorsed. I'm not *quite* as persuaded as some of my colleagues in the civil liberties community that this should be an absolute dealbreaker this specific instance—provided that the FISC also reviews some basic

information about the initial fruits of a query, which the HPSCI bill does *not* require or provide for.

I say that because in this case, each directive will yield the records of dozens or hundreds of contacts for every selector explicitly specified. Moreover, the FISC will rarely have much ex-ante basis for second guessing the government's "reasonable suspicion" determinations. Suppose instead the FISC were to review directives relatively quickly *after* issuance *along with* a very rough statistical precis of the information obtained: How many unique contacts are identified at the first and second hop? How many of these belong to United States persons, to the extent this can be easily determined? While permitting ex-post approval does increase the risk that some requests will "slip through the cracks," or that some information will be obtained on an inadequate basis, a more robust review provision than the HPSCI bill provides might at least give the FISC some basis for catching dubious determinations of suspicion. If a particular seed selector is pulling in an unusually large number of first-hop contacts, or if the purported cell phone of a Pashtun goatherd is primarily calling numbers in the 202 area code, the FISC might at least be motivated to ask for some supporting documentation. That's not to say the trade is necessarily worth making—and again, what I've described is emphatically *not* provided for in the HPSCI bill—but it's at least worth considering.

(C) The Bottom Line

Let's sum up. First, the HPSCI bill's seemingly broad prohibition on bulk collection turns out to be riddled with ambiguities and potential loopholes. The fuzzy definition of "specific identifiers" leaves the door open to collection that's extremely broad even if not completely indiscriminate. Because the provision dealing with "call detail records" applies only to §215 and the provision dealing with "electronic communications records" excludes telephony records, the law *does not* bar the bulk collection of telephony records under FISA provisions other than §215. The prohibition on non-specific acquisition of other communications "records" *probably* does not preclude bulk collection under the FISA pen register provision that was previously used for the NSA Internet metadata dragnet. And, of course, none of these prohibitions apply to National Security Letters. If the government wanted to keep collecting metadata in bulk, it would have plenty of ways to do so within the parameters of this statute given a modicum of creative lawyering—at least if the FISC were to continue being as accommodating as it has been in the past.

Second, something *like* the novel authority created here *may* well be necessary to enable fast and flexible acquisition of targeted records without dragnet collection. However, once we get down to details—and even leaving aside the question of ex-post versus ex-ante judicial approval—this authority is in some respects broader than either the current §215 telephony program, the president's proposal, *or* the pre-Snowden understanding of the FISA business records authority. Critically, it eliminates the required link to a predicated investigation—which, in the case of U.S. persons, must be for counterterrorism or counterespionage purposes.

While this would at least presumably put an end to the current dragnet collection of telephony metadata, it is not at all clear how seriously it would constrain the government's bulk collection of records on the whole. In some respects, there is at least a colorable argument that the new

authority could expand the scope of government collection in some respects. Given the government's track record on this front, it is probably not excessively paranoid to suspect that any such loopholes and ambiguities are likely to be exploited.

About the Author

[Julian Sanchez](#) is a research fellow at the Cato Institute and contributing editor for Reason magazine. Follow him on twitter @normative.