

# THE LEAHY- SENSENBRENNER LANGUAGE ON BACK DOOR SEARCHES IMPROVES BUT DOESN'T ELIMINATE THE BACK DOOR

As the top Intelligence Community lawyers have made clear, the IC maintains it can search US person data incidentally collected under Section 702 without any suspicion, as well as for the purposes of making algorithms, cracking encryption, and to protect property.

The Leahy-Sensenbrenner bill tries to rein in this problem. And its fix is far better than what we've got now. But it almost certainly won't fix the underlying problem.

Here's what the law would do to the "Limitations" section of Section 702. The underlined language is new.

(b) Limitations

(1) IN GENERAL.—An acquisition

(A) may not intentionally target any person known at the time of acquisition to be located in the United States;

(B) may not intentionally target a person reasonably believed to be located outside the United States if a significant purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(C) may not intentionally target a United States person reasonably believed to be located outside the United States;

(D) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(E) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(2) CLARIFICATION ON PROHIBITION ON SEARCHING OF COLLECTIONS OF COMMUNICATIONS OF UNITED STATES PERSONS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), no officer or employee of the United States may conduct a search of a collection of communications acquired under this section in an effort to find communications of a particular United States person (other than a corporation).

(B) CONCURRENT AUTHORIZATION AND EXCEPTION FOR EMERGENCY SITUATIONS.—

Subparagraph (A) shall not apply to a search for communications related to a particular United States person if—

(i) such United States person is the subject of an order or emergency authorization authorizing electronic surveillance or physical search under section 105, 304,

15 703, 704, or 705, or title 18, United States Code, for the effective period of that order;

(ii) the entity carrying out the search has a reasonable belief that the life or safety of such United States person is threatened and the information is sought for the purpose of assisting that person; or

(iii) such United States person

has consented to the search.' [all emphasis my own]

Basically, this section adds a restriction on searching for US person communications, except in an emergency or with the consent of that person (this language might make it easier to require the government to search on this collection for discovery).

I'm particularly interested in the bolded language, which replaced "the purpose" with "a significant purpose." It suggests Pat Leahy and Jim Sensenbrenner either suspect or know the government is getting around the clear restriction on reverse targeting by claiming that if targeting the US person isn't the only reason they are collecting the data, they can go ahead and do it, even if targeting the US person is part of why they are targeting the foreign person. I especially like the fix because the government vastly expanded the use of FISA information – even to the point of using it to look for crimes like rape they could use to coerce people to turn informant for the government – by using changing the limits on FISA to "a significant purpose."

Back atcha spooks!

So until the Executive finds some new loophole it can use to get around the clear intent of the law, this new language should limit searches on US person data collected under Section 702 to real emergencies (or at least emergencies the government is willing to document as such).

However, that's only true of data collected under Section 702.

As Raj De made clear on Monday, the Executive also conducts back door searches on data collected under EO 12333.

MR. DEMPSEY: Okay. Am I right, the same situation basically applies to information collected outside of FISA? So FISA collection inside the United

States, 12333 collection outside the United States, but those communications collected outside the United States might include collections to or from U.S. citizens, U.S. persons, and again, those can then be searched without even a RAS type determination, is that right?

MR. DE: I think, yeah, I don't know if we've declassified sort of minimization procedures outside of the FISA context, but there are different rules that apply. [my emphasis]

If the IC collects data "legally," it maintains, they can search it, even without suspicion of wrongdoing, and their use of it is only limited by minimization procedures (which, in the case of E0 12333, only need to pass muster with the Attorney General, not a Judge).

And, as Russ Feingold summarized the views of the Executive Branch 5 years ago – including those of Keith Alexander – if Congress limits dragnet collection in ways the Executive doesn't like, they'll just do what they want under Article II.

SEN. FEINGOLD: Well, here's the problem. If we're going to pass this statute, whether it's a good idea or a bad idea, it sounds like it won't be the only basis on which the administration thinks it can operate. So in other words, if they don't like what we come up with, they can just go back to Article II. That obviously troubles me.

Way back during the initial debate over bring Bush's illegal dragnet under the purview of FISC and Congress, the Executive Branch made clear they refused to be bound by that.

And therefore, we can be certain – especially given the increasing globalization that has happened since 2007, when they said this – that

if this language passed, the IC would just collect even more data under E.O. 12333 so they could go on reverse targeting Americans.

It seems several more things would need to happen to protect against back door searches. First, Google and Yahoo and other multinational providers would need to find some way to prevent NSA from stealing their data. And, Congress would need to start drafting laws that recognize "foreign" is no more distinct than "domestic" was in 2007 when Congress started changing the law to account for technological changes here. Alternately, Courts need to start treating this suspicionless searches through petabytes of global communications as a Fourth Amendment violation.

Right now, Americans have very little protection for their communications that can, in any way, be deemed foreign. And while Leahy-Sensenbrenner is an improvement, it will not fix the problem.