KEITH ALEXANDER'S SECRET LIE: RETENTION AND DISTRIBUTION OF DOMESTIC ENCRYPTED AND HACKING COMMUNICATIONS?

As I noted in my last two posts, Keith Alexander has admitted that the classified lie Mark Udall and Ron Wyden accused him of telling "could have more precisely described the requirements of collection under FISA Amendments Act."

He then goes onto repeat the many claims about Section 702, which are different forms of saying that it may not collect information on someone knowingly in the US.

Which leads me to suspect that the lie Udall and Wyden described is that the program can retain and distribute domestic communications, which are defined as "communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition."

The minimization procedures actually describe four kinds of domestic communications that can be distributed with written NSA Director determination. Three of those — significant foreign intelligence information, evidence of a crime imminently being committed, and threat of serious harm to life or property — were generally known. But there is a fourth which I think is probably huge collection:

> Section 5(3)
>
> The communication is reasonably believed to contain technical data base information, as defined in Section 2(i), or information necessary to understand or assess a communications security

> vulnerability. Such communication may be provided to the FBI and/or disseminated to other elements of the United States Government. Such communications may be returned for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.
>
> a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any time period during which encrypted material is subject to, or of us in, cryptanalysis.
>
> b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is five years unless the Signal Intelligence Director, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements,

Technical data base information, according to the definitions, "means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes."

In other words, hacking.

Encrypted communications and evidence of hacking have secretly been included in a law purportedly about foreign intelligence collection. And they can keep that information as long as it takes, exempting it from normal minimization requirements.

To be clear, the government still has to get the

communication believing (according to its 51% rule) that it has one foreign component. But if Keith Alexander says so, NSA can keep it, forever, even after it finds out it is a domestic communication.

Update: Here's the July 2012 letter to Clapper. Here's Clapper's August 2012 response — the good bits of which are all classified.