DAILY KOS

And one other thing about NSA collection... Retention

August 13, 2013

Pursuant to the Issue of Turnkey Totalitarianism this is from a pretty lively debate on the subject featuring Spencer Ackerman and Robert Gibbs from All In.

Ackerman talks mainly about the 702 Loophole that could allow U.S. persons to be queried in the database. I'm still checking by that seems to me to be consistent with what the Guardian Reported, and some weeks ago I read in the FISA Court Opinion released by Snowden, that shows that when looking at Foreign Data U.S. Data is inadvertently discovered, the NSA & FBI are allowed to use exigent circumstances to analyze that data when a Crime or National Security Issues arise.

Secret minimization procedures dating from 2009, published in June by the Guardian, revealed that the NSA could make use of any "inadvertently acquired" information on US persons under a defined range of circumstances, including if they held usable intelligence, information on criminal activity, threat of harm to people or property, are encrypted or are believed to contain any information relevant to cybersecurity.

This of course does confirm something Senator Wyden has been hinting at for some time but has been unable to say without violating Security Rules.

However there was something else that Robert Gibbs brought up toward the end of the discussion that I want to highlight:

The bigger Constitutional Issue that has been brought up is the validity of the *Building the Data Haystack* itself, even if the government limits itself on the ability to search that Haystack until it has gained a FISA warrant to do so.

As Ackerman says the Patriot Act only allows the authority to *collect* information pursuant to a specific warrant or inquiry, whereas the function of the PRISM and others similar systems seems to depend on *Pre-collection of Everything* then the use of a Warrant to limit and control the sifting and searching of that data.

From Section 215 of the Patriot Act

(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person

is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

What were talking about here are something called *Administrative Warrants* that the FBI Director can issue without a Judge, including a FISA Judge. Unfortunately I wasn't able to find the section that Ackerman says that this limits this to "collection" because the verbiage actually says "Obtain" not "Collect".

In this case it would be the FBI *obtaining* the information from the NSA Data Haystack pursuant to a National Security Investigation. In general I don't have a problem with this idea, I'm more troubled by the fact that this can be done without the FISC and that it can includes a Non-Disclosure requirement that doesn't allow someone receiving such a warrant to even contact a lawyer to protect themselves.

Julian Sanchez of the Cato Institute makes a strong argument that there's never been a truly documented case of a plot that has been foiled by the NSA data, and that there is no legitimate justification for having this massive collection effort.

Sanchez:

There's never been any intelligible case made that they need a builk database like this, in any of the cases they've talked about. In everyone of these cases it would have been better to get a more targeted search. Whenever the Inspector General or the Senate with real access to the classified information look at it. Oops it turns out that Fusion Centers never produced any useful information. Oops, Warrantless Wiretaping was an incredibly limited utility, it wasn't pivotal in the cases they said it was.

Of course in this case he's talking about the Bush Era version of the program that didn't involve the FISA Court *AT ALL* and didn't have any minimization procedures in place. That was then, this is now.

The director of the National Security Agency insisted on Tuesday that the government's sweeping surveillance programs have foiled some 50 terrorist plots worldwide in a forceful defense echoed by the leaders of the House Intelligence Committee.

Army Gen. Keith Alexander said the two recently disclosed programs – one that gathers U.S. phone records and another that is designed to track the use of U.S.-based Internet servers by foreigners with possible links to terrorism – are critical in the terrorism fight.

Intelligence officials have disclosed some details on two thwarted attacks, and Alexander promised additional information to the panel on thwarted attacks that the programs helped stop. He provided few additional details.

We'll just have to wait to see how accurate these claims turn out, and whether their validity evaporates in the same way that Bush's claims did.

The suggested alternative to getting the information from the Big Haystack would be to let the *data stay at it's source* rather than build the comprehensive stack - and it's on this point that Gibbs confirms something here that I've long suspected.

They don't keep that data very long. Gibb states this at the 8:22 mark in the video.

Gibbs:

Let's be clear Ezra, AT&T and Verizon They don't keep your records so if you're going to go find somebody and go backwards several years how are you going to do that? You have to have some collection... and you can't listen to a conversation in the past. You have to have some collectable data, with which to trace those numbers.

Service providers like Verizon & AT&T don't retain the data for more than a few weeks or months. From a technical standpoint, *it's not otherwise possible* to reconstruct this information if it no longer exists on the original computer systems. In other words, if the NSA weren't building and collecting this Haystack of data going back as far as two years (under the limits set by the FISA court) *there can't be an alternative set of little Haystacks* stored on the Verizon, AT&T and Microsoft servers because they don't have the capacity.

Now if we want to have government *force* all of those providers to each keep two years of their information just so, in case they need to, the DOJ can search those contacts and conversations for information on terrorists - that's an entirely new discussion to be had.

But as of right now, they can't do it.

So although there is shaky legal grounds for this, as a DBA I've always understood that *technical* advantage of organizing and gathering the data in a comprehensives way. It makes *sense* to do this, the problem of course is keeping that data safe for unauthorized and illegitimate use.

And can anything that potentially powerful *ever* be keep completely safe?