NSA is 'bamboozling' lawmakers to gain access to Americans' private records – agency veteran

Published time: 12 Jun, 2013 04:27
Edited time: 12 Jun, 2013 04:59

Get short URL

Error loading player:
No playable sources found

Bill Binney (Still from RTAmerica video) / RT

American citizens hoping to change the way the NSA monitors their everyday activities have little hope of recourse, longtime agency veteran Bill Binney told RT. He said the way the Patriot Act is interpreted is the a big first step toward totalitarianism.

RT:*I'm sitting here with Mr. William Binney -- he's a thirty-two year veteran of the NSA who helped design a top-secret program that he says broadly changed Americans' personal data. And he actually helped crack those codes, and enter into this. He's now a whistleblower. Mr. Binney, thank you so much for joining me. So first of all, let's talk about the latest information that has come out from this NSA spying on Americans.*

Tags
Conflict, Scandal, SciTech, Protest, Politics, Internet, Information Technology, USA, Security, Hacking

Bill Binney: Well, first of all, the FISA warrant that was issued to the FBI to get the data from Verizon… that's been going on, according to the paper anyway, since 2007. And this is like being renewed every three months. So if you look at the top-right corner of that order, it's 13-80 -- that means it's the 80th order since this year of 2013. So when you start to say, so what are the other 79 orders? You can figure other companies. And this is like the second order of 2013, for each company. So that maximum -- you would divide 80 by two, and the maximum number of companies that could be involved in this order would be 40. But I'm sure that there are other things, that they have other orders they are issuing than just this kind, for the service providers, or the telecoms.

RT:*So let's talk about the nine Internet companies that said that they are part of this PRISM program. Should Americans really be surprised at this*?

BB: Well I'm not, that's for sure. But I would point out that the NSA had deployed Naris devices in its court documents submitted by Mark Klein, documenting the NSA room in the San Francisco At&T building where they had Naris devices in a splitter that basically duplicated the fiber-optic lines and would send them down two paths. All the information went down two directions: one of them went down the Naris devices in the NSA room. And so those Naris devices could take everything off of that fiber-opti ssemble a milli y could get from one well as other

Where to watch Schedule

Alleged US security officials said NSA leaker, journalist should be 'disappeared' – report

NSA leak fallout: LIVE UPDATES

Assange on Snowden: He's a hero, we've been in contact

places in the world, so that's an awful lot of data to try to manage. So they need to do things like build Bluffdale to plan for the future so they have lots of storage for all this data.

RT:*So how far down the rabbit-hole are we*? *Are we really just at the tip of the iceberg in terms of their spying with this PRISM program coming out in the Verizon records*?

BB: Tim Clemente, who is an ex-FBI agent, came on CNN a week or two ago, and he said that any digital data wasn't safe, and that the intelligence community and the FBI had ways of getting back to it. And he was specifically talking about the phone call between one of the [Tsarnaev] brothers and his wife. And if his wife didn't tell the FBI what they talked about in that phone call, that they had ways of getting back to that and transcribing and getting the information. So that's telling you what they've got recorded – then they extend it and have digital data. That means all kinds of email, all kinds of Twitter kind-of things, anything going across the fiber-optic lines, as well as the public switch telephone network.

RT:*So we're not talking billions of pieces of information here, we're talking trillions.*

BB: We're talking trillions, yea. My estimate with phone calls and emails jointly would be on the order of 20 trillion for the last 12 years.

RT:*How can we even manage such a thing*? *They're saying, with this PRISM program for instance, we have one lawmaker after another supporting it, saying it helps thwart at least one terrorism attack. How would trillions of emails and trillions of bits of data help find one terrorist attack*?

BB: My personal view is that the intelligence community is bamboozling Congress and the administration. They are telling them that they have to do this in order to find the bad guys in the networks, and that's just absolutely false. You don't have to do that. There are ways and means to do that, and I left that ability and capability with them, and they just threw it away. So instead they just opted to collect everything they could about everybody in this country, and one of the reasons that they would want to do that – the only one I could think of is they wanted to be able to leverage anybody in this country. For example, we can take the case of the IRS and the tea party, and the harassing they're doing there. One of the people that's being harassed was giving testimony in front of Congress. And they said, which I thought was quite revealing, was that they had a question from the IRS that asked, "what Is your relationship with this other person?" And they gave the name. Well how would they know that unless they knew the communications community of that person? So that means you're getting back to this program where they're pulling all the records of phone calls and emails and everything together and seeing who that person worked with. And on top of that it gave them the ability to pull together the entire tea party. So you would know everybody that's involved in the tea party, peripherally or centrally.

RT:*Now this new PRISM program says that the agents who are employing need to have a 51 percent confidence that it's a foreign agent, a foreign person. Can you talk about that accuracy, how can we guarantee it, and is 51 percent even enough*?

BB: Well that's another joke *[laughs].* These are all jokes. They expect people to believe this. There are two parts: one is the public switch, the PSTN – public switch telephone network, and the other is the Internet, or the World Wide Web. On the one side you have phone numbers. Now these phone numbers, whether they're your landline phone or your mobile phone or your satellite phone, [they] all connect into this public switch telephone network, and those numbers are unique in the world. And you're talking about switches that are routing these communications from one point in the other to another. And they have to know exactly where to send it. And so you know exactly where it went and exactly where it's coming from. So there's no question that we shouldn't have fairly 99.9999 percent accuracy on identifying that – unless something happens and they have electronic blip and they lose part of the information.

And the other thing is, on the World Wide Web – here again they have attributes that are part of the world wide system that identifies those people that are uniquely in the world, like the IPV4, the IPV6. You know, addresses that are assigned by the IANA in the five regions of the world. And that clearly tells you, if you don't have that, then every device – whether it's a switch, a server or a computer – had a MAC number. That's a machine access code that identifies you uniquely in the world. And the same would be true in using username and service provider combinations, like williambinney@comcast.net, something like that. Those kind of attributes identify where you are and where you're coming from.

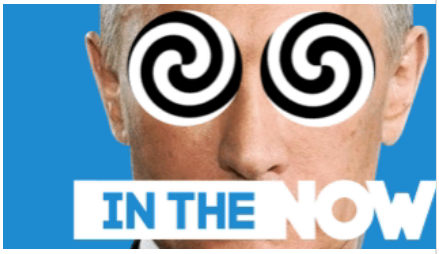
RT:*So let's talk about the companies, the nine Internet companies that are involved in this. They say that they didn't know that this was possibly happening under their watch. First of all, is it even possible that they didn't know*?

BB: Certainly it's possible that some of the people in these companies didn't know, but I find it hard to believe that that wasn't already agreed to, that somewhere in the company the COO or the CEOs knew and agreed to this kind of access. Because it's hard to believe that they could not notice that they're being drained of information 0 that's pretty difficult.

RT: A*nd you have, on the other hand, lawmakers on Capitol Hill. We went out as a group with RT and we interviewed people on the streets. And one after the other, a person said that they are not only OK*

Edward Snowden: The man who exposed PRISM

NSA to continue global surveillance program



with this type of surveillance – but that they actually encourage it if it thwarts terrorism. So talk about this debate, this debate between civil liberties and national security – should it be either or, in this case?

BB: No, you can have both. The point is that you can filter out all the domestic communication that isn't connected in any way with any terrorist – or even close to a terrorist, like two degrees of separation in the communications network or communities you're building. You can reduce it to that, and if you're not in that zone, then all your data is thrown away, and that would eliminate 99.99 percent of the US population and the world. But they don't do that. So that's where they're getting back to the idea and bamboozling Congress and the administration to suggest they need to collect it all to figure it out. That's simply false.

RT:*So what can we really do to protect ourselves, is there anything we can do to protect ourselves here*?

BB: Not really, there's not really anything you can do, except to fire everybody in Congress and the administration and elect new people that will do a constitutionally acceptable job.

RT:*And speaking of Congress, how much do they know, how could they be OK with it*? *How did so much of this just start coming out with the Verizon leaks? With this PRISM? How are we just finding out about this in an administration that touts transparency*?

BB: Well, it's because it's not transparent. They have secret interpretations of laws and they're doing this in secret and not telling anybody. I mean Sens. Wyden and Udall had been complaining about this for several years now. So they were on the intelligence committee. Committees had an idea of what was going on, but the rest of Congress didn't have the foggiest idea. And for example, they're using section 215 of the Patriot Act to say it's ok for them to get that – that had to do with the commercial held data. Like if I send an email, my service provider would be holding it -- so that's a third party and they say that's a commercial third party. [They say] all that data is legitimate for them to collect, when in fact it isn't – even under the Patriot Act. 'Cause the Patriot Act was designed, according to Rep. Frank Sensenbrenner, who wrote the Patriot Act – he was saying today that it was intended to resolve issues with foreign intelligence of threats from terrorists. Well, domestic communications is not foreign, and there's no threat there – there's no relationship of threat, there's no probable cause or any indication that any of the data they're collecting about the vast majority of US citizens is in any way related to terrorism.

RT:*That was going to be my next question. What does the Patriot Act mean to American freedoms*?

BB: It means we don't have any. It's setting up a totalitarian state. When the government has that much information, they can use the IRS to intimidate people or anything else. They can send the FBI at people, like they did to me and some others. So that's the power that the government has – they have the power of the gun and the force and if they have the knowledge about you then they can start to use that against you – especially if you don't agree with the policies that they're setting up.

RT:*So lets go back to the Foreign Intelligence Surveillance Act – FISA, as a lot of us know it. The first word of that act is "foreign", and that was built back in the 70's and it applied to foreign enemies then. But in the 30, 40 years since, we've seen it apply to Americans more times than not. Will we see the same thing happen with PRISM*?

BB: Yes, absolutely, that's what's going on, that's what's been going on for seven years with the PRISM program. But even before that, back to 2003, the Naris devices were collecting that data. Now what that meant was they didn't have enough Naris devices to collect everything, so they had missing bits of it – like they might get 80 percent of the emails sent, but not all of them. In order to get them all, they have to go to the service provider, which stores them all for a certain amount of time, and then have a warrant to request to get them. So that will fill in the gaps that they are missing – that's why they're doing it. I would point out the warrant, which says the request is being made by the FBI. But the order says send the data to the NSA. So that tells you the relationship between the FBI and the NSA: the NSA has the algorithms to process it and package it and make it look pretty and reduce the problem to the point where FBI agents can look into it easily and analyze and manage data faster and be more complete at what they look at. So, that shows you the level of cooperation between the FBI and the NSA.

RT:*Now, when you were working for the NSA, you had hoped to create a program that's similar to PRISM for our foreign enemies. Did you know about PRISM then*?

BB: No. I left the NSA in 2001 at the end of October, and the PRISM program, according to the paper anyway, started in 2007. So I didn't know about that, but that data was very simply filtered out using techniques that… if this was a US citizen, you'd throw that data away. If this was a foreigner that wasn't within two zones, or two degrees of separation, in close proximity to a bad guy doing bad things, we wouldn't even look at them. We'd throw it all away. And that meant we'd have reduced the problem of all the massive amounts of data to a manageable amount. So we wouldn't need to build Bluffdale or any other large storage sights – we could easily manage the storage as well. And if you collect all of that, that means wherever you collected it, then you have to transport it from there to your storage. We eliminated that communications cost [with the algorithm].

RT:*So is it as simple as just getting rid of that algorithm that helped them draw it out and sort through it*?

BB: That algorithm would of course be able to eliminate that data, yeah, if they adopt it.

RT:*Finally, just working for the NSA in the past – do you regret that, or does it give you the knowledge of what the NSA has done so that you can do it and report to people in the future*?

BB: I didn't regret anything I was doing because there were real issues, real threats and real potential threats that we had to try to discover to see if we could diplomatically avoid them. That was a very positive effort against the real potential threats. It had nothing to do with collecting data or information about innocent people across the world. I didn't regret doing any of that. The problem was they turned that against everybody, and that's where I have a problem.

RT:*Bill Binney is a 32-year veteran of the NSA-turned whistleblower. Thank you so much for joining us, we appreciate your time.*