GlobalResearch
Center for Research on Globalization

Inside the Puzzle Palace: interview with NSA whistleblower Russell Tice

By Julian Sanchez
Global Research, January 23, 2006
Reason 23 January 2006

Region: USA
Theme: Police State & Civil Rights

(Interview conducted by Reason)

In December, New York Times reporters James Risen and Eric Lichtblau commandeered the news cycle with the revelation that President Bush had approved a program of warrantless wiretaps of domestic-to-international communications by the super-secretive National Security Agency. Days later, they disclosed that the NSA's electronic eavesdropping may have been far more extensive than initial reports suggested, involving the harvesting of enormous volumes of telcommunications data for analysis.

One of their sources was former NSA insider Russell Tice, who earlier this week told ABC News that the communications of millions of Americans might have been vacuumed up in one of a number of classified NSA programs. "If you picked the word 'jihad' out of a conversation," Tice explained, "the technology exists that you focus in on that conversation, and you pull it out of the system for processing."

Critics say Tice is a paranoid, embittered by his May 2005 firing from the agency. Tice says he's a whistleblower who was punished for speaking up—and now wants to make sure Congress hears what he has to say about what he believes are unconstitutional activities carried out in the name of the War on Terror. The programs that have been made public so far, according to Tice, are just the tip of the iceberg. Assistant Editor Julian Sanchez spoke with Tice—and anyone else who may have been listening—by telephone this week.

REASON: You've described technologies capable of sifting through vast numbers of communications and pinpointing very specific information that intelligence analysts are looking for. What can you say about how that kind of technology is being used?

Tice: I can't say how an intelligence agency uses it, because that would be classified. Then the FBI would have shackles and cuffs waiting on me real soon, so I have to be careful what I say. But we can talk about the technologies and we can use hypotheticals and we can use wiggle words.

If you wanted to, you could suck in an awful lot of information. The biggest constraint you're going to have is the computing power you need to do it. You need to have some huge computers to crunch that kind of stuff. More than likely you're talking about picking it up in a digital format and analyzing it depending on how the program is written depending on whether it's audio or digital recognition you're talking about, the computing power is phenomenal for that sort of thing. Especially if you're talking about mass volumes, if you're talking about hundreds of thousands of, say, telephone communications or something like that, calls of people just like you and me, like we're talking now.

Then you have things like, and this is where language specialists come in, linguists who specialize in things like accents and inflections and speech patterns and all those things that come into play. Or looking for key phrases or combinations of key words within a block of speech. It becomes, when you add in all the variables, astronomical.

REASON: Do you have a sense of the scale that's possible, how many phrases and conversations it might be possible to filter?

Tice: Technically it's limitless. It's like, you know what a Boolean logic line is? **[Yes.]** Think of a Boolean logic line with these sorts of parameters in your normal Boolean, built on these filtering parameters. As long as the software is designed to handle however long the Boolean string is in this case, then you have the computing power and the other equipment to crunch the information to put it through the filtering process. Technically you can do as much as you want. It's going to cost you a lot of money and you're going to have to buy some big computers and other equipment, bit synchronizers and that sort of thing, monitoring error rates.

You have to be careful to overdo it, because if you overdo the situation, you'll saturate your bit error rate. So in our hypothetical situation, you could write a program to do this, but you wouldn't be able to filter enough, say. Ultimately you would have to tweak it over time; you would analyze what your output was and say "no, we're getting too much garbage, so we need to focus on this particular filter or this particular item, to be able to winnow it down to where you want it to be."

You run the risk the other way of omitting information you may have wanted, which is where you need specialists, who know exactly the information you want, to work with the software engineers and the language specialists to make sure that everyone's working in sync so that you get the what you want. Normally a linguist or a software engineer isn't the intelligence analyst or intelligence specialist who knows the nitty-gritty of the intelligence or the information you're looking for.

REASON: There's always a problem looking for low-frequency events in a large population, even with a very good filter. How big a problem do you think false positives are?

Tice: It's going to be a huge problem. Huge. That's going to be your number one concern insofar as false positives are ultimately your error rate. The ultimate goal, more than likely in our hypothetical scenario, is to filter this thing down enough so that you can put it into human analysts' hands. The ultimate filter, the ultimate computer, is the human brain.

REASON: How can you minimize that problem in a system like this?

Tice: Some sort of a built in quality control, and automate that as much as you possibly can. So you're always analyzing the output of this and tweaking it as much as you can. The key in this sort of processing is to get the machines and the computers to do as much of it for you as you can as effectively as you can. Garbage in, garbage out. So all your players have to be working in sync to get something like this together.

REASON: Do you see a shift in signals intelligence toward more intensive

computer filtering, so there's more and more information processed, but less seen by human beings?

Tice: I've thought about this for a while, and as I said, I can't tell you how things are done, but I can foresee it, especially with what we've seen now. We're finding out that NSA conducted surveillance on U.S. citizens. And FISA could have been used but wasn't, was sidestepped. No one even made the attempt to see if they had a problem they could have fixed through FISA.

That would lead one to ask the question: "Why did they omit the FISA court?"

I would think one reason that is possible is that perhaps a system already existed that you could do this with, and all you had to do is change the venue. And if that's the case, and this system was a broad brush system, a vacuum cleaner that just sucks things up, this huge systematic approach to monitoring these calls, processing them, and filtering them—then ultimately a machine does 98.8 percent of your work. What you come out with from a haystack is a shoebox full of straw. Once you have that, you have people that can look at it.

Now here's an interesting question: If this approach was used, and hundreds of thousands if not millions of communications were processed in that manner, and then if and when the truth ever came out, a lawyer—and I think lawyers are going to be arguing semantics in this case—the argument could be made, well, if a machine was doing the looking and the sucking in, it doesn't matter because that's not monitoring until a human looks at it.

REASON: What prompted you to step forward now?

Tice: Well, I've known this for a long time and I've kept my mouth shut…

REASON: You're referring to what James Risen calls "The Program," the NSA wiretaps that have been reported on?

Tice: No, I'm referring to what I need to tell Congress that no one knows yet, which is only tertiarily connected to what you know about now.

REASON: What aspect of that, within the parameters of what you're able to talk about, concerned you?

Tice: The lack of oversight, mainly—when a problem arose and I raised concerns, the total lack of concern that anyone could be held accountable for any illegality involved. And then these things are so deep black, the extremely sensitive programs that I was a specialist in, these things are so deep black that only a minute few people are cleared for these things. So even if you have a concern, it's things in many cases your own supervisor isn't cleared for. So you have literally nowhere to go.

REASON: So there's a problem of inadequate channels of communications to raise concerns?

Tice: Yeah, zero channels of communication because you're talking about information so closely held that even within a large organization like the Agency, only a handful of people may know. The director would know, maybe the deputy director, the chief of security, maybe one level-supervisor, maybe my own supervisor—and these are all management people. And then you have one person, me, the worker bee who does the work, writes the reports, goes into the field, does the liaison work, makes the phone calls. I was the nitty-gritty detail guy.

REASON: What about the Intelligence Community Whistleblower Protection Act?

Tice: The interesting thing about the ICWPA that came up in my case, the NSA put it right in bold print: They said even if Mr. Tice made a protected disclosure under the ICWPA, there is no provision in the ICWPA to punish or hold responsible the agency doing the retaliation, in this case the NSA. So even though the law says it's protected, there's no teeth in the law to do anything to the NSA. So they can screw you over with impunity, and even if someone did determine you had a claim, there's nothing there to punish them. In the writeup I had, they showed their contempt for that in the way they wrote up the piece of nonsense in their defense. The ICWPA as far as I know has only had something like two disclosures in the years it's been in existence. You know why? Because any intelligence officer knows if you do this, your career is done. They will find something to use to revoke your security clearance, which is what they did with me, which destroys your career in the intel field, makes you unemployable forever. I will never be an intelligence officer ever again; I will never be able to work as a contractor for a firm that does intelligence community contracts.

REASON: What would you like to see Congress do?

Tice: Pass some laws with some teeth. Congress is real quick to say "oh, this is intelligence and we don't want to compromise their methods." Well, fine. But they have the mechanism in [Equal Employment Opportunity] to discuss things. My case could very easily be, and was easily, discussed in an unclassified manner, as to their reasons for firing me. It's disingenuous on their part to throw out that national security nonsense because they don't want to give up their power to screw people over; it's a means of intimidation.

REASON: What action would you have them take about the programs that concern you?

Tice: I'd like for there to be some internal… First of all, I don't want this stuff to leak out. I'm not going to tell you or anyone in the press anything that's classified, especially about these programs. Because for the most part they're extremely beneficial to the security of our citizens, programs that are worth their salt. The problem is that you can have abuses within that system, and there's no oversight. So ultimately what we need is some adult supervision of these programs, maybe some bipartisan group of senior intelligence elders who've retired from their normal intelligence jobs. These senior officials could be on a senior advisory review board to deal with these sort of things in an unbiased, non-partisan manner in a very tightly-held way, but nonetheless look at these cases and act as some sort of judge as to how things need to be addressed.

REASON: Are you at all sympathetic to claims that the *New York Times*' reporting on NSA surveillance may have harmed national security?

Tice: In my case, there's no way the programs I want to talk to Congress about should be public ever, unless maybe in 200 years they want to declassify them. You should never learn about it; no one at the *Times* should ever learn about these things. But that same mechanism that allows you to have a program like this at an extremely high, sensitive classification level could also be used to mask illegality, like spying on Americans. And spying on Americans is illegal unless you go to a FISA court. It's the job of the FBI to conduct operations against Americans with the proper court warrants—not that I have a very high opinion of the FBI.

With [James Risen's] book, someone has come across, and basically reported, a crime. It just so happens that somebody put some super-duper clearances on it to mask the fact that a crime was being committed. Now we're claiming after the fact, to do some damage control, that "oh no, now the terrorists know." Come on, let's be rational about this. Do we think that the terrorists are just plain stupid? Do we think that, especially after 9/11, the terrorists aren't smart enough to think that maybe the United Statesmight be interested in the communications they conduct and how they conduct them? Even if you believe there's some negativity in that information coming out, which I think is a totally disingenuous claim, but even if you think there's some merit to that, when you weight it against the fact that you're breaking the constitutional rights of American citizens, the scale on the right side incredibly outweighs any claim on the other side.

REASON: How scrupulous is the general culture of the NSA about avoiding spying on Americans?

Tice: As a signals intelligence officer, kids who go right out of college and work for the NSA, this is drilled into you, especially when you're young: You will not do this. This is number one of the NSA's Ten Commandments: You will not spy on Americans. Even after you've had all those introductory briefings when you're a new employee, for the rest of your career, at least twice a year they call you in for a briefing, and this is always covered. "You will not do this," they shake their fingers at you. "If you do this you can be thrown in jail." And all of a sudden you find out the people who've been shaking their fingers are doing what they're telling you is against the law and coming out with some cockeyed nonsense excuses for why everything's OK. It's sort of like having your parents drill it into you not to smoke cigarettes or do drugs or whatever, and then after you're a good little boy coming home from school at 15 and finding your parents out on the balcony doing all that.

Fear rules the day right now. For the most part, people know, NSA employees know, that this is wrong, that this is illegal. In many cases they feel betrayed by their own leadership, by [former NSA Director Gen. Michael] Hayden, [NSA Director Lt. Gen. Keith] Alexander, and by [Deputy Director] Bill Black.

And the president—I'm a Republican, I voted for this guy. I've always given him the benefit of the doubt. I didn't like the PATRIOT Act; I don't like a lot of what I've seen. But I've always felt that this president, in his heart, felt he was doing his best to protect the American people. I thought PATRIOT, and throwing the key away on Jose Padilla, were unconstitutional, but I've always given him the benefit of the doubt. I'm certainly hoping that he's been misled, and that if a broad-brush approach was used that the president wasn't aware of it or didn't understand the ramifications, that hundreds of thousands if not millions of Americans could have their rights violated. But if that happened and the president knew totally the extent of it, and everything we're hearing now is just damage control from the White House… Well, some time ago, we impeached a president for cheating on his wife, which as far as I'm concerned should've been between his family, his wife, and if he believes in one his God upstairs. When it comes to high crimes and misdemeanors, knowingly and willingly doing *this* and then being arrogant about it and saying we're going to continue doing it—I would certainly think falls into that category of high crimes.

REASON: Some polls suggest that most citizens aren't terribly concerned about

these programs.

Tice: People think it's not going to affect them. They think it's against the bad people, it's to protect our national security. Maybe it's against the law, but it's just the bad people, just to keep the terrorist from blowing up my neighborhood dam. But if those people find out it was hundreds of thousands or millions, and they were swept up into it and the government was listening to their conversation with their doctor…. Now all of a sudden it affects them personally. Right now I don't think people see how it affects them. Though even if it were just these few thousand people that have been talked about, nonetheless it's wrong. There's no reason the two thousand warrants could not have been done through the FISA court. The question is: Why wasn't it done?

Julian Sanchez is an assistant editor of Reason. He lives in Washington, D.C.

The original source of this article is Reason

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Julian Sanchez

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca