From Democracy Now | Original Article

Watch Part 1 of Interview with William Binney

William Binney describes how his former agency has built a massive system to track, monitor and record phone and Internet communications of U.S. citizens and people around the world. Binney resigned from the National Security Agency in 2001 to protest growing domestic surveillance. He was a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network. He was one of the two co-founders of the agency's Signals Intelligence Automation Research Center. He resigned after the Sept. 11 attacks. In 2012 he gave his first ever television interview to Democracy Now!

AMY GOODMAN: This is *Democracy Now!*, democracynow.org, *The War and Peace Report*. I'm Amy Goodman. Our guest is William Binney. He served in the National Security Agency for almost 40 years, including a time as director of the NSA's World Geopolitical and Military Analysis Reporting Group, a senior
NSA
crypto-mathematician, largely responsible for automating the agency's worldwide eavesdropping network. He was one of the two co-founders of the agency's Signals Intelligence Automation Research Center, resigned after the September 11th attacks, concerned about the increasing surveillance of the American people.

We are getting response to the massive series of releases and exposés from *The Guardian*new spaper and
The Washington Post
of information released by a 29-year-old information technician named Edward Snowden, who worked for Booz Allen Hamilton, a military contractor, within the National Security Agency in Hawaii. In response to these revelations about surveillance, President Obama spoke on Friday and defended the NSA's surveillance program, suggesting they help defend the country against terrorist attacks.

PRESIDENT BARACK OBAMA: I came in with a healthy skepticism about these programs. My team evaluated them. We scrubbed them thoroughly. We actually expanded some of the oversight, increased some of the safeguards. But my assessment and my team's assessment was that they help us prevent terrorist attacks. And the modest encroachments on privacy that are involved in getting phone numbers or duration without a name attached and not looking at content, that on, you know, net, it was worth us doing. That's—some other folks may have a different assessment of that. But I think it's important to recognize that you can't have 100 percent security and also then have 100 percent privacy and zero inconvenience. You know, we're going to have to make some choices as a society. And what I can say is, is that in evaluating these programs, they make a difference in our capacity to anticipate and prevent possible terrorist activity.

AMY GOODMAN: William Binney, you worked for the NSA for almost 40 years. You're reading all of this information that's been released right now about the surveillance abilities of the NSA
and what they're doing right now. Can you respond to President Obama?

WILLIAM BINNEY: Yes. Personally, I've had the view for any—for quite a number of decades, that the Congress and the administration have been—have been fed by the intelligence community what I call technobabble. In other words, they're being bamboozled into thinking a certain way, that they have to do this in order to get terrorists. And that's simply false. There's a simple way to do it that would protect people's privacy and not invade anybody's telephone records or email. And that's to say, if you have a terrorist, and he calls somebody in the United States—I call this the two-degree principle—that's one degree of communication separation. Then you look at that as a target, and you collect that, and then you look also at the person in the United States and who they talk to. That could represent the—that's a zone of suspicion that would, in effect, be basically a support network for that person inside the country. That defines your terrorist relationship, and that's how you look at that. And the rest of the communication of the U.S. people don't mean anything, as relevant, and none of that's relevant to what's going on there. And you also have to look at the jihadi-type sites, those that advocate jihad or violence and so on, and you see who is accessing those sites. That's easy to monitor that, and it doesn't invade anybody's privacy that's been absolutely doing nothing of—that should be in any way considered suspicious.

AMY GOODMAN: On Friday, President Obama also refuted claims that the intelligence community is listening to telephone conversations.

PRESIDENT BARACK OBAMA: When it comes to telephone calls, nobody is listening to your telephone calls. That's not what this program is about. As was indicated, what the intelligence community is doing is looking at phone numbers and durations of calls. They are not looking at people's names, and they're not looking at content. But by sifting through this so-called metadata, they may identify potential leads with respect to folks who might engage in terrorism. If these folks—if the intelligence community then actually wants to listen to a phone call, they've got to go back to a federal judge, just like they would in a criminal investigation. So, I want to be very clear. Some of the hype that we've been hearing over the last day or so—nobody is listening to the content of people's phone calls.

AMY GOODMAN: Is that true, William Binney? You worked at the NSA for almost 40 years.

WILLIAM BINNEY: Well, it's pretty—it's pretty much true, yes. I think they are—my sense is that they are just looking at a target list. They have a target list that they input to the telephone network and use the switches to detect these phone calls going across the network and then download those to recorders and transcribe that. So that's what they're—I think that's what they're doing. But what Edward Snowden was talking about was having access to that network. What that meant was he could load—and what he was basically saying, he could load the attributes of anyone he wanted to target into the target list, and then that would start doing, executing and collecting all the information about them, including the content, and recording it, too. So they could—and someone would have to transcribe it, but they could, and all of that content for phones, as well as email, would be stored and collected in the base.

AMY GOODMAN: Let's go back to what Edward Snowden had to say.

EDWARD SNOWDEN: You don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they can use the system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.

AMY GOODMAN: William Binney, your response to Edward Snowden, the 29-year-old NSAwhi

stleblower?

WILLIAM BINNEY: Yeah, that's pretty much correct. I mean, when you pull in the call records at the rate of three billion a day over 12 years and you graph them, what that means is you now have the total communications communities that everyone has in the world, or in the United States, basically. And at that point, that shows you all of your relationships. And that's part of what he was talking about. The other part was the Narus devices that they deployed starting, I think, around 2003 onto the fiber optic networks, were capturing the emails and voice over IP, and that was being stored. And so, then that's why they have to—that's why they have to build places like Bluffdale in Utah, that big storage facility, because they're collecting so much data. The content is the real—the content is really the bulk that needs to be—that they're storing. The call records and just graphing the relationships is a pretty simple thing to do, and it doesn't take that much—you could put that in one room of storage capacity.

AMY GOODMAN: Bill Binney, could you say a little more about Bluffdale, this site in Utah that's being built right now? I don't think most people are aware of it.

WILLIAM BINNEY: Well, what they're putting together there in Bluffdale is a million-square-foot storage facility, of which only 100,000 is really going to have equipment to store data. But the rest of it, the peripherals, then are power generation, cooling and so on. So, but in there, there's 100,000 square feet of storage capacity. And at current capabilities that are advertised on the web with Cleversafe.com , they can put 10 exabytes in about 200 feet—square feet of storage space in 21 racks. What that means is, when you divide that out, is you—that even at current capacity to store information, that's five zettabytes that they can put in into Bluffdale. And if you—and my estimate of the data they would be collecting, which would include the targeted audio and perhaps all of the text in the world, that would be on the order of 20 terabytes a minute—or, yeah, 20 terabytes a minute. So if you figure out from that how much they could collect, it would be like 500 years of the world's communications. But I only estimated a hundred, because really they want space for parallel processors to go at cryptanalysis and breaking codes. So—

AMY GOODMAN: William Binney, we didn't speak to you last week before PRISM came out, or we spoke to you before the revelations about
PRISM
, so I wanted to ask you about them today. I mean, these revelations are coming out almost every day right now, where the
NSA
obtains access to the central servers of nine major Internet companies, including Google and

Yahoo! and Microsoft and Apple and Facebook,
The Guardian
then exposing how the president had ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for U.S. cyber-attacks. Could you respond one—each one of those, first
PRISM
, and what that allows the
NSA
to do, and what you think should be done about that?

WILLIAM BINNEY: Well, first of all, what they were talking about there is the Internet and the communications going across the Internet. And that really—the access of that data really started back with Mark Klein when he exposed the deployment of the Narus devices on the web. That was giving them the content of everything on the fiber optic lines. That was the collection that they had. Now, when they had that—deploy those collection sites all around, they don't—still don't get all of the data, so they have holes in their collection. They may get 80 percent, basically, of what's being passed on the web. But by going to those companies and saying—they store everything they serve, so they've got a—if you aggregate them together, they've got a complete picture of what's on the web. And so, going there allows
NSA
then to fill in the gaps that they're missing from their real-time collection. So, that's the objective that I think is going on there. But, I mean, it's—in the meantime, that's collecting all the data on U.S. citizens again. And if they went back to use the two-degree principle, they could, again, protect U.S. citizens and still find all of the terrorists in the world. So, I mean—

AMY GOODMAN: Bill Binney, can you comment on this period we're going through right now, when you have Bradley Manning on trial at Fort Meade, which is the national headquarters of the National Security Agency? He faces life in prison or possibly death. Then you have this young man, Ed Snowden, who, 29 years old, understands the stakes, says he understands he may never be home again, now in Hong Kong, the last we know. The significance of what is coming out right now? And then, Julian Assange, you know, holed up in the Ecuadorean embassy in London—

WILLIAM BINNEY: Yeah.

AMY GOODMAN: —afraid he might be extradited to the United States and face the same fate as perhaps Bradley Manning.

WILLIAM BINNEY: Well, all of that, plus all of the previous prosecutions of whistleblowers is really an attempt to intimidate the governmental workforce and the contractor workforce that's associated with them, so that they don't compromise things that the government doesn't want the public to know. And so, that's really their objective, and that's why they're coming after whistleblowers and people who turn over documentation of government programs and trying to, of course, give them as much of the penalty of the law that they can do and—if they can get a hold of them.

AMY GOODMAN: Which brings us to you, Bill Binney. Talk about what you attempted to do, in terms of getting out information, sounding the alarm right after 9/11, when people were willing to give a lot of leeway, that, you know, you've got to trade privacy for security, but what you felt, being inside the National Security Agency for the decades that you were, and the shift after 9/11, what you faced, as well as your other colleagues.

WILLIAM BINNEY: Well, it was pretty hard for me to believe that my agency, that I had supported for so many years, and the country, of course, and the laws that we had, including the USSID 18 that has—which was our guiding documentation internally in NSA about not spying on U.S. citizens—when they started doing that after 9/11, it was just hard for me to believe they did it, but it—the evidence—I mean, I had direct evidence that they were doing it, so I just couldn't—I couldn't stay there. I couldn't be a party to that. And what I did after that was tried—I went to the intelligence committees first to try to get them alerted to it, so they would try—address it. I mean, their responsibility was to prevent the intelligence community from spying on U.S. citizens, based on the FISA laws. And after that, when that didn't work, I even tried, with Diane Roark and others, to address this issue to the Chief Justice Rehnquist of the Supreme Court. But we weren't able to do that. And so, eventually, I tried the—as well as Kirk Wiebe and I, we both tried to get to the Department of Justice inspector general's office and alert them to this and say there are ways to do it without violating all the U.S. citizens' privacy. But that wasn't what the government wanted to do. I mean, when Qwest, the CEO of Qwest, was approached in February of 2001—that was before 9/11—to give over customer data, it was all—it was still targeting domestic spying, and that was call records they were trying to get from that. So, the—

AMY GOODMAN: And talk about that for a moment, Bill, the former Qwest CEO Joe Nacchio, the only head of a communications company to—the only head of a company to demand a

court order or approval under
FISA
.

WILLIAM BINNEY: Yes, and the consequence for him was they targeted him, and now he's in prison. So, I mean, they succeeded in prosecuting him. But what it told me was that the intent from the beginning was to do domestic spying, accumulating information and knowledge about the U.S.—the entire U.S. population. So I thought of that as a J. Edgar Hoover on super steroids, you know? It wasn't that he had information and knowledge to leverage just the Congress. You have information and knowledge to leverage everyone, judges included, in the country. So, that's why I got so concerned. I tried to work internally in the government to get people to do something about it, but that whole process failed. So what it did was it alerted them to what I was doing, and they targeted me with the FBI, and they attempted to falsely prosecute me. Fortunately, I was able to get evidence of malicious prosecution every time, so they finally backed off trying to prosecute me.

AMY GOODMAN: If you would briefly, though I don't like to have you relive this, tell us what actually happened to you, with the FBI raiding your home.

WILLIAM BINNEY: Well, they came in, and there were like 12 FBI agents with their guns drawn, and came in. My son opened the door, let them in, and they pushed him out of the way at gunpoint. And they came upstairs to where my wife was getting dressed, and I was in the shower, and they were pointing guns at her, and then they—one of the agents came into the shower and pointed a gun directly at me, at my head, and of course pulled me out of the shower. So I had a towel, at least, to wrap around, but—so that's what they did.

And then they took me out and interrogated me on the back porch. And when they did that, they tried to get me—they said they wanted me to tell them something that would be—implicate someone in a crime. And I said, well, I didn't—I thought they were talking about someone other than the President Bush, Dick Cheney and Hayden and Tenet, so I said I didn't really know about anything. And they said they thought I was lying. Well, at that point, "OK," I said, "I'll tell you about the crime I know about," and that was that Hayden, Tenet, George Bush, Dick Cheney, they conspired to subvert the Constitution and the constitutional process of checks and balances, and here's how they did it. And I talked about program Stellar Wind, all the data coming in, about how they managed to graph it and also how they bypassed the courts. They didn't tell the courts about this program, and they didn't solicit any approval from the courts. And they also only told four people initially in Congress, that were the—they were the chiefs and deputies of the Intelligence Committee. That was on the House. That was Porter Goss and

Nancy Pelosi. I don't remember the Senate side. But when you do that and—I mean, Senator Rockefeller, when he got briefed into those programs in 2003, said he wasn't capable of understanding any of it, because he wasn't—he wasn't a technician, he wasn't a lawyer, so he couldn't do anything about it. That was in his handwritten note to Dick Cheney. So, I mean, it was clear they were doing something that was unconstitutional and against any number of laws that existed at the time.

AMY GOODMAN: William Binney, what most surprised you about the latest series of revelations that come from Edward Snowden?

WILLIAM BINNEY: Well, the only surprise I got—I mean, the PRISM program, I had assumed was going on anyway. But the court order that was published that showed the—it showed the serial number at the top, on the top right side of it. It was 13-80. That meant it was the 80th order of 2013 of the FISA court. And if that order was typical of all those other 79, which was authorizing them—or ordering them to turn over records that would—to NSA, even though it was the FBI doing the request, it shows you the relationship between FBI and NSA. It's really close, and they're depending on NSA to do their processing. But what it is, what that tells me, that serial number told me that, gee, if all those orders addressed individually every quarter—this was the second quarter of 2013—then there would be, at a minimum, 40 companies involved in this activity. So, it would be telcoms—it would be a mix of telcoms and Internet service providers.

AMY GOODMAN: You know, there's been a lot made of the document that shows that Verizon is handing over its information.

WILLIAM BINNEY: Right.

AMY GOODMAN: But that's just because that's the document they have.

WILLIAM BINNEY: Right.

AMY GOODMAN: Do you assume we're talking BellSouth, we're talking AT&T and the other corporations?

WILLIAM BINNEY: Yeah, plus the Internet service providers, and that would add up to 80 orders from that court that—this year so far, for two quarters. So, each company would get an order each quarter to do that. So that's—you have to divide 80 by two. And that's the minimum, OK?

AMY GOODMAN: Edward Snowden worked for Booz Allen Hamilton. That's a military contractor. He worked in the NSA offices in Hawaii. He had also worked at the CIA. He had also worked with Dell. He's only 29 years old. In fact, actually, he didn't graduate from high school, but a very smart, young, intelligent technician. Can you talk about that relationship between the military contractors and the NSA? I mean, how this young man has this kind of access, it's very similar to Bradley Manning sitting in the desert in Iraq.

WILLIAM BINNEY: Well, I think it gets back to what Glenn Beck was—or, Glenn Greenwald was talking about: the outsourcing of the intelligence process to contractors. I mean, that's what's been going on for about at least 10 years. They've been outsourcing the dependency on contractors to run their programs. So that means these contractors all have access to all this information about U.S. citizens in all these programs that they're running. I mean, they're depending on them to support it and make it happen and operate so their analysts can access the information.

AMY GOODMAN: How many people have access to this information, if Edward does, 29 years old, can do all the things that he said he could do sitting in an office in Hawaii?

WILLIAM BINNEY: Well, if you're counting government employees, that could be thousands, depending on how many—how many agencies are involved in looking into that data. I mean,

the FBIcertainly is, and the fusion centers they have around the—around the country, with the FBI integrated, are probably all part of that, too.

AMY GOODMAN: Speaking of the FBI, in 2008, actor Shia LaBeouf appeared on *The Tonight Show with Jay Leno*. During the interview, he talked about an FBI agent showing him a recorded conversation from two years prior to meeting him.

SHIA LABEOUF: I remember we had an FBI consultant on the picture telling me that they can use your ADT security box microphone to get your stuff that's going on in your house, or OnStar, they could shut your car down. And he told me that one in five phone calls that you make are recorded and logged. And I laughed at him. And then he played back a phone conversation I had had two years prior—

JAY LENO: Come on.

SHIA LABEOUF: —to joining the picture. The FBI consultant. And it was like one of those—it was one of those phone calls—it was like, you know, "What are you wearing?" type of things.

JAY LENO: Really?

SHIA LABEOUF: Yeah, so it was—it was mad weird, but—

JAY LENO: Can we—no, wait. So you mean they had a record of you from—

SHIA LABEOUF: Two years prior to me joining the picture.

JAY LENO: —even being associated with the movie?

SHIA LABEOUF: With the movie.

JAY LENO: Well, that seems creepy.

SHIA LABEOUF: It's extremely creepy.

AMY GOODMAN: Shia Labeouf. It was 2008 that he was speaking on *The Tonight Show*, so I think he was talking about the film
Eagle Eye
that had just come out. William Binney, your response?

WILLIAM BINNEY: Well, you know, I would assume that they—they, for whatever reason—I'm not sure, I didn't see that movie, but he may have been saying things that were objectionable to the administration, and so they put him on the target list for monitoring. The same thing would happen to—happened to Laura Poitras. I mean, she was, because of her movies, showing—you know, *My Country, My Country*, basically—I think that was the one that did it, that—

AMY GOODMAN: About Yemen.

WILLIAM BINNEY: This—that one was about Iraq and the Iraq War and how the Iraqis were surviving and how they—in the war zone.

AMY GOODMAN: Right.

WILLIAM BINNEY: So, I think—I don't—I think if you're doing something like that, that—

AMY GOODMAN: And then she went on to do a film about Yemen.

WILLIAM BINNEY: Right. So, if you're doing something that irritates or is against what the government wants to be expressed to the American public, then you can become a target. That's what that's saying.

AMY GOODMAN: Now, Edward Snowden used the codename VERAX, which is Latin for "truth teller." Do you see Edward Snowden as a truth teller, as a whistleblower?

WILLIAM BINNEY: Well, I think he's telling the truth. I mean, he's got the documentation to back it up to, so I think certainly what he's saying is correct.

AMY GOODMAN: Do you applaud what he has done?

WILLIAM BINNEY: I wouldn't have done it that way, OK, because I would have tried to work the system first. So, but, I mean, if you make the decision, you have to suffer the consequences. And with the government we have, they're going to be pretty harsh, I think. So, they're going to try to do whatever they can to him.

AMY GOODMAN: Bill Binney, *Bloomberg Businessweek* recently disclosed how a secretive unit inside the National Security Agency called Tailored Access Operations conducts massive

cyber-espionage on overseas computer networks, the Pentagon hackers harvesting nearly 2.1 million gigabytes every hour, the equivalent of, oh, like hundreds of millions of pages of text. Do you know about this?

WILLIAM BINNEY: Well, I think they would refer to that as active attack on your computer, and it's like hackers. You know, it's this—that's how you can—what they're doing is going across the network and going through your weaknesses or holes in your operating system and then getting into your computer and then looking at whatever data you have in there, selecting it out, and using your unused CPU to send it back to themselves. So, that's—that's pretty much what they're doing. That's, of course, what the Chinese are doing to us, so that's—and I'm sure other countries are doing it—the Israelis, the Russians, all of them, you know? So that's standard hacking into the system that we hear about, too, so...

AMY GOODMAN: For people who have not been following the story of whistleblower after whistleblower after whistleblower, and it goes on from there, who have been cracked down on under the Obama administration, can you tell us about the coterie of folks who worked at the NSA
, like you? And also, then, would you do this again, what you've done, considering what you've gone through?

WILLIAM BINNEY: Well, first of all, let me take you—the population at NSA, about 85 percent of them, I think, are ISTJs on the Myers-Briggs scale, and they're very strong introverts, you know? They have a very focused job to do. Breaking a crypt system or something is a very focused effort. You—it's really intense. So it's really something that's really compatible with their character. And so, when something happens and they see things happening to people who get involved, like myself or others, they get afraid. And being introverts, they even go further as—further into themselves and staying isolated. So, that's—that's the primary character of people. And the others, the others are probably part of it and believe that it's the correct thing to do. And they don't try to find a reasonable, constitutionally acceptable, legally acceptable way to do the—to achieve the objectives that they want. They simply felt that they had to go to the far—the other far side of the spectrum and get as much as they can about everybody they can.

AMY GOODMAN: Would you have done again what you did?

WILLIAM BINNEY: Uh, I probably wouldn't now. But if I were—if I had—if I wasn't—if I was facing a similar problem, I would still try to work a system—if it was a different system, I would

still try to work within the system to try to get it changed. But if that didn't work, I'd probably do exactly what I'd done with the other situation, in NSA. So, I probably would still stay in character and try to get it worked out internally and then—and try to stay within the system, initially anyway.

AMY GOODMAN: Well, William Binney, I want to thank you very much for being with us, NSAw histleblower, 40 years almost at the agency, for a time NSA's World Geopolitical and Military Analysis Reporting Group, deeply concerned about the level of surveillance of Americans, ultimately was almost prosecuted,
FBI
gun at his head in the shower, as well as his wife and child, but in the end he did not face prosecution as others have under the Espionage Act. This is
Democracy Now!
, democracynow.org,
The War and Peace Report
. I'm Amy Goodman.