Display full version

MONDAY, APRIL 23, 2012

More Secrets on Growing State Surveillance: Exclusive with NSA Whistleblower, Targeted Hacker

In part two of our national broadcast exclusive on the growing domestic surveillance state, we speak with National Security Agency whistleblower William Binney and two targeted Americans: Oscar-nominated filmmaker Laura Poitras and hacker Jacob Appelbaum, who has volunteered for WikiLeaks and now works with Tor Project, a nonprofit organization that teaches about internet security. Binney left the NSA after the 9/11 attacks over his concerns about the agency's widespread surveillance of U.S. citizens. He describes how the FBI later raided his home and held him at gunpoint and notes there is still no effective way of monitoring how and what information the NSA is gathering on U.S. citizens and how that data is being used. Click here to watch part one of our special report. [Includes rush transcript]

TRANSCRIPT

This is a rush transcript. Copy may not be in its final form.

AMY GOODMAN: We turn to part two of *Democracy Now!'s whistleblower*william">national broadcast exclusive on the growing domestic surveillance state and the Department of Homeland Security's efforts to spy on dissident journalists, whistleblowers and activists.

We play more of our interview with National Security Agency whistleblower William Binney. He was a key source for James Bamford's recent exposé in *Wired Magazine* about the NSA, how the National Security Agency is quietly building the largest spy center in the country in Bluffdale, Utah. Binney served in the NSA for close to 40 years, including a time as technical director of the NSA's World Geopolitical and Military Analysis Reporting Group. Since retiring from the NSA in 2001, he has warned the agency's data-mining program has become so vast it could, quote, "create an Orwellian state." In 2007, the FBI raided Binney's house. An agent put a gun to his head. His appearance on *Democracy Now!* on Friday marked the first time Binney spoke on national television about surveillance by the National Security Agency. He revealed the agency collected vast amounts of data on communications between U.S. citizens.

Juan González and I also interviewed two people who have been frequent targets of government surveillance. Laura Poitras is the Oscar-nominated filmmaker, and Jacob Appelbaum, a computer security researcher who has volunteered with WikiLeaks. Poitras is the director of documentary films, *My Country, My Country*,

about Iraq, and *The Oath*, about Guantánamo and Yemen. Both Poitras and Appelbaum have been repeatedly detained and interrogated by federal agents when entering the United States. Their laptops, cameras, cellphones have been seized. Presumably, their data has been copied. The Justice Department has also targeted Appelbaum's online communications.

I started by asking Jacob Appelbaum about his work and how being targeted for surveillance has impacted him.

JACOB APPELBAUM: I work for a nonprofit, and I work for—

AMY GOODMAN: Explain the nonprofit.

JACOB APPELBAUM: The nonprofit is the Tor Project, TorProject.org. It's a nonprofit dedicated to creating an anonymity network and the software that powers it. It's free software for freedom, so that everybody has the right to read and to speak freely. No logins, no payment, nothing. It's run by volunteers. And I also work at the University of Washington, which technically is a government institution, as a staff research scientist in the Security and Privacy Research Lab.

And how has it changed my work? Well, like Laura, I don't have important conversations in the United States anymore. I don't have conversations in bed with my partner anymore. I don't trust any of my computers for anything at all. And in a sense, one thing that it has done is push me away from the work that I've done around the world trying to help pro-democracy activists starting an Arab Spring, for example, because I present a threat, in some cases, to those people. And I have a duty as a human being, essentially, to not create a threat for people. And so, in a sense, the state targeting me makes me less effective in the things they even, in some cases, fund the Tor Project to do, which is to help people to be anonymous online and to fight against censorship and surveillance.

JUAN GONZÁLEZ: I'd like to ask, William Binney, the impact of having devoted your entire working life to an agency—that is, to protecting the national security of the United States—to have that very agency then attempt to turn you into a criminal and to view you as a criminal, the emotional toll on you and your family of what's happened the last few years?

WILLIAM BINNEY: Well, I guess, first of all, it was a very depressing thing to have happen, that they would turn their—the capabilities that I built for them to do foreign—detection of foreign threats, to have that turned on the people of the United States. That

was an extremely depressing thing for me to see happen internally in NSA, that was chartered for foreign intelligence, not domestic intelligence.

And I guess that simply made it more important for me to try to do things to get the government, first of all, to correct its own criminal activity, and I did that by going to the House Intelligence Committees. I also attempted to see Chief Justice Rehnquist to try to address that issue to him, and I also visited the Department of Justice Inspector General's Office—after Obama came into office, by the way, to no avail. I mean, that was before the 2009 joint IG report on surveillance.

AMY GOODMAN: Which said?

WILLIAM BINNEY: Basically it just said you need to have better and more active monitoring of these surveillance programs. It didn't say anything else. So that just simply did absolutely nothing, because the oversight that's given to the intelligence community is virtually nonexistent from Congress. I mean, all—they are totally dependent, because they have no way of really knowing what's happening inside the agencies that are involved. Unless they had people who would come forward and tell them—like me, for example—they would not know those things.

AMY GOODMAN: Bill Binney, can you compare today's surveillance to John Poindexter's Total Information Awareness, who was head of DARPA—and you can explain what that military agency was—the outcry then, forcing ultimately the Bush administration to say, "It is shut down. We're ending Total Information Awareness"?

WILLIAM BINNEY: Well, here's how I viewed Poindexter's efforts. He was actually pushed out as a test, to test the waters in Congress to see how they would be receptive to something they were already doing. In other words, that process of building that information about everybody getting total information was already happening. And they threw Poindexter out with DARPA, which is the base—an advanced research group. They fund advanced research programs, and that was one of the things they were saying they were doing, but it was actually already happening. And the question was, would it be acceptable to Congress, because they were keeping it very closely held in Congress under the—calling it a covert program. So, that makes it—that would make it a process to find out what the reaction would be, if they exposed to Congress what they were already doing.

JUAN GONZÁLEZ: But the NSA is such a huge agency, and there are so many career people in that agency. Your concerns cannot be yours

alone. There must be many within the agency who are deeply troubled by what's going on.

WILLIAM BINNEY: Oh, yeah, I'm sure there are. I mean, I know a number of them that are. But they're still—they're so afraid to do anything. I mean, they've seen what happened to us. They sent the FBI to us. So they're afraid of being indicted, prosecuted. And even if you win the case, if you're indicted, you still lose, because you've had to hire a lawyer and all, like Tom did and we did.

AMY GOODMAN: Tom Drake.

WILLIAM BINNEY: Right, Tom Drake. And so, you lose any way you speak of it. When they have unlimited funds to do whatever they want and you don't, they can indict you on any number of things, like they tried to do with us.

AMY GOODMAN: They didn't indict you, though.

WILLIAM BINNEY: They drafted an indictment, but they didn't—they didn't actually do it, because I found evidence of malicious prosecution. And they dropped it.

AMY GOODMAN: How?

WILLIAM BINNEY: Well, the indictment was drawn up against all of us who were on the IG report, and also Tom Drake, because we all met, plus some others, at the Turf Valley Club, and they had all our emails and all of our data to show that we were doing that. Plus they had the view graphs that we prepared there. And their whole objective there was, how could we incorporate to attack Medicare/Medicaid fraud? And so, what we were doing was preparing a joint teaming paper that would be a kind of a incorporation papers. They called that the "conspiracy paper." They called it a conspiracy, and we were conspiring to do something. But they didn't—they thought they had all the exculpatory evidence, and they didn't, because there were two other people there that weren't—that had never had a clearance, and they were going to participate in this, in this development, so they had all the data, too.

And when I found out, because they told our lawyer that they were preparing to indict us on that as a conspiracy, why, I went through and pulled all the data together. And since Tom had been indicted at that time, and I knew his phone was tapped, so I—by the FBI—I decided I would give him a call and tell him what all the evidence is of malicious prosecution, so that I was speaking to the FBI people, and they would

pass the information along to the DOJ, that would say, "Hey, we know this is malicious prosecution. You had the emails that listed the agenda, what we were going to discuss at the Turf Valley Club. You also had all of the slides that we prepared at the Turf Valley Club. And, oh, by the way, if you need to find out when they were prepared, you go in to click on the file, go down to properties, look in the properties and see the date and time that the file was created, and that's when we were at the Turf Valley Club. So it was direct evidence of what we were doing there. Plus there were two other people that were there that they didn't have a grudge against, so they weren't targeting, and they never talked to them at all about what the meeting was about." So I said, "This is all evidence of malicious prosecution. And you need, Tom, to tell your lawyer about this," because I was telling the FBI that we're going to notify all our lawyers what you're doing. So, and after that phone call, we never heard about the Turf Valley Club again. That was dead.

AMY GOODMAN: Tom Drake then, though, faced espionage charges.

WILLIAM BINNEY: They created—yeah, they created other charges.

AMY GOODMAN: They said he had aided the enemy, etc. Ultimately, the case went away.

WILLIAM BINNEY: Those were all fabricated charges, yeah.

AMY GOODMAN: William Binney, federal aviation regulators have acknowledged dozens of universities and law enforcement agencies have been given approval to use drones inside the United States. The list includes Department of Homeland Security, Customs and Border Protection, various branches of military, defense contractor Raytheon, drone manufacturer General Atomics, as well as numerous universities, Police departments with drone permits include North Little Rock, Arkansas; Arlington, Texas; Seattle, Washington; Gadsden, Alabama; and Ogden, Utah.

WILLIAM BINNEY: Well, that's simply another step in the assembly of information. This is the visual part of the electronic information they're collecting about people. So here's your visual part. I mean, you could collect on phone—the cellphones as you move around, and then you can watch them now with a drone.

AMY GOODMAN: And it's not just the NSA who can gather phone information.

WILLIAM BINNEY: No, this—

AMY GOODMAN: Police departments now.

WILLIAM BINNEY: Right. Actually, I think it's shared, because if you—if you go back and look at Director Mueller's testimony on the 30th of March to the Senate Judiciary Committee, he responded to a question when he was asked the question of "How would you prevent a future Fort Hood?" He responded by saying that "We have gotten together with the DOD and have created this technology database." He called it a "technology database." Utah will be included in that, I'm sure. And—

AMY GOODMAN: Meaning Bluffdale.

WILLIAM BINNEY: Yeah, right.

AMY GOODMAN: Where they're building this massive data center.

WILLIAM BINNEY: Its storage, yeah. And he said, "From this technology base, with one query, we can get all past and all future emails. So we only have to make one query to get it." That means he gets a target, puts the target in, goes into the base, pulls all past ones, and as they come in, then he gets all future ones. So, that says they're sharing it across the legal—with the legal authorities, so...

JUAN GONZÁLEZ: But then also having these private defense contractors and universities, I mean, you're talking about a potential in terms of—not only of people gathering information, but of malicious use of that information by—

WILLIAM BINNEY: Yeah, you want to see if your wife is cheating on you? OK, you could do that, yes. That's right. There's a—that's the hazard of assembling all this kind of data. It's not just the government misusing it, but it's also people working in it, looking at it, and using it in different ways. They have no effective way of monitoring how people are using that information. They don't.

AMY GOODMAN: You can get information under the Freedom of Information Act about your FBI files, but can you get information about what the NSA has on you? And explain the difference between the CIA and the NSA. I think a lot of people don't even realize there's this far larger intelligence agency in the United States than the CIA.

WILLIAM BINNEY: Yeah, it's about three to four times as large, yeah. The difference is that the primary focus of CIA is supposed to be human intelligence, a human espionage, you know, like spies, recruiting sources around the world, and so on, whereas NSA's responsibility is electronic intercept and electronic—analysis of

electronic communications, to form intelligence from what they're either saying or how they're acting, to assess threat. And CIA is to take the people input side, the human input side. That's their charter, anyway, so... But they also do some of their own intelligence gathering, that there's kind of some overlap there, which is, I guess, a part of their charter also. I've not really looked at the CIA charter that much. But so —but I do know they do some of that. But they're primarily focused on human intelligence.

JUAN GONZÁLEZ: And has there been any historic conflict or competition between the NSA and the CIA, as you often have seen that —

WILLIAM BINNEY: Yes.

JUAN GONZÁLEZ: —more recently with the FBI and the CIA?

WILLIAM BINNEY: It's not—it's not historical. It's continuous. It is a continuous competition. It's—the barrier for sharing, the way I would put it, is they're hesitant to share knowledge and information, because then that's sharing power, and you no longer control that kind of input to higher authorities for decision making. So when they do that, that's like releasing knowledge and releasing their power to others. And that's a barrier for them.

AMY GOODMAN: Jacob Appelbaum, I asked you before how people can protect themselves. I remember you mentioned, when they took your computer, the authorities at the border, there wasn't a hard drive in it. Explain what people can do.

JACOB APPELBAUM: Well, I think one thing that is important is to know that if you're being targeted, these people, they're, you know, in the weapons industry. It turns out that they also have the ability to break into computers. So, if you're being targeted, you have to take a lot of precautions. For example, there's a bootable CD called "Tails," and the idea is you run Linux, and all your traffic routes over Tor, so you don't have something like Adobe Flash trying to update itself, and then the NSA or someone else gets to perform what's called a "man in the middle" attack. Instead of using Gmail, using something like Riseup. I mean, after their server was just seized, I think kicking them some cash is probably a good thing. They provide mutual aid for people all around the world to have emails that are not just given up automatically, or even with a court battle. They try to encrypt it so they can't give things up. So people can make choices where their privacy is respected, but also they can make technical choices, like using Tor, to ensure, for example, that when data is gathered, it's encrypted and it's

worthless. And I think that's important to do, even though it's not perfect. I mean, there is no perfection in this. But perfection is the enemy of "good enough."

AMY GOODMAN: How do you download Tor, T-O-R?

JACOB APPELBAUM: You go to TorProject.org, https://www.torproject.org. And the "S" is for "secure," for some value of "secure." And you download a copy of it, and it's a web browser, for example. And the program, all put together, double-click it, run it, you're good to go.

AMY GOODMAN: You can even Skype on it?

JACOB APPELBAUM: You—I would really recommend using something like Jitsi instead of Skype. Every time you use proprietary software—

AMY GOODMAN: "Jitsi" is spelled...?

JACOB APPELBAUM: J-I-T-S-I. So, every time you use proprietary software, you have to ask yourself, "Why is this provided to me for free?" And now that Microsoft is involved with Skype, the question is: Doesn't Microsoft have some sort of government leaning on them, say the U.S. government, to give them so-called lawful interception capabilities? And of course the answer is going to be yes, right? If you log into Skype on a computer you've never used before, you get all your chat history. Well, why is that? Well, that's because Skype has it. And if Skype can give it to you, they can give it to the Feds. And they will. And everybody that has that ability will. Some will fight it, like Twitter. But in the end, if the state asserts it has the right to get your data, sometimes without you even knowing that that's happening, they're going to get it, if they can get it.

So we have to solve these privacy problems with mathematics, because it's pretty hard to solve math problems with a gun or threat of violence, right? No amount of violence is going to solve a math problem. And despite the fact that the NSA has got a lot of people working on those math problems, you know, podunk cops in Seattle, for example, they're not going to be able to do that, and the NSA is not going to help them. Now, they may have surveillance capability. They may have IMSI catchers. They might have automatic license plate readers. They have an incredible surveillance state. They're still not the NSA.

And even if they are sharing information, what we want to do is make whatever information they would share worthless, especially if it's

encrypted. So if your browsing is going over Tor, at least if someone is watching your home internet connection, they don't see that you're looking at *Democracy Now!*'s website. They don't see that you're checking your Riseup email. They see that you're talking to the Tor network. And there's a lot of value in that, especially because your geographic location is hidden. So when you log into Gmail—let's say you still use Gmail—but you don't want Gmail to have a log of every place you've been, you use Tor, and Gmail sees Tor, and anyone watching you sees Tor. And that's really useful, because it means that they don't get your home address, they don't know when you're at work. You make the metadata worthless, essentially, for people that are surveilling you.

JUAN GONZÁLEZ: I think you may have just gotten a lot of customers for Tor, for Project Tor.

AMY GOODMAN: When your computer or phones are taken at the airport, do you use them again?

JACOB APPELBAUM: I never had my phones returned to me, and I can't talk about that. And my computer, I had—I mean, I can't remember where I put it, so, I mean, the government back door that's probably in it is hopefully in safety somewhere.

AMY GOODMAN: The *New York Times* blog says, "Companies that make many of the most popular smartphone apps for Apple and Android devices — Twitter, Foursquare and Instagram among them — routinely gather the information in personal address books on the phone and in some cases store it on their own computers. The practice came under scrutiny Wednesday by members of Congress who saw news reports that taking such data was an 'industry best practice.'" Jacob Appelbaum?

JACOB APPELBAUM: Sounds like a data Valdez waiting to happen.

AMY GOODMAN: What gives you hope, William Binney? You worked in a top-secret agency for close to 40 years. You quit soon after 9/11 because you saw that the agency was spying on the American people, and you had helped develop the program that allowed this to happen.

WILLIAM BINNEY: Well, the only thing that gives me hope is programs like this or *Wired* articles that Jim Bamford would write about this activity, to get the word out so that people can be aware of what's happening, so in a democracy we can stand forward and vote, in some way, as to what we want our government to do or not to do, and

what kind of information we want them to have or not have.

JUAN GONZÁLEZ: And are there any members in Congress that you see waging a good fight around this issue?

WILLIAM BINNEY: Well, Senators Wydall *sic* and Udall are, so—Wyden and Udall, they are. And there are others. They're just not speaking up. Of course, the problem is, you see, they can't tell you what their concern, because—

LAURA POITRAS: Well, why? Why can't they tell you? I mean, what would be the repercussions if you're in Congress?

WILLIAM BINNEY: Well, because what happens when—if they did, for example, they would lose their clearance immediately and be off the committees.

AMY GOODMAN: Talk about the Gang of Eight, what they know, who they are.

WILLIAM BINNEY: Well, according to Cheney, it originally started with a Gang of Four. And then, after the 2004 objections in the DOJ, then it expanded to the Gang of Eight. The Gang of Four initially was the majority and minority leader of the Intelligence—House Intelligence Committee and the Senate Intelligence Committee, the HPSCI and SSCI. Then, after the—and that, on the House side, that was Chairman Goss and Nancy Pelosi, initially, in 2001. I don't remember the other two on the Senate side. And then it expanded in 2004, it expanded to the Gang of Eight, which added—on top of those four, it added the senior—the majority and minority leaders of the House and the majority and minority leaders of the Senate.

AMY GOODMAN: So, Jacob Appelbaum, Laura Poitras, your response to what these civilian elected leaders know?

LAURA POITRAS: Well, it's shameful. I mean, I don't know how they're going to explain it to their grandkids, right? I mean, I think this whole post-9/11 era is—it's indefensible, right? I mean—and so, if the risk is losing one's clearance, is that really a risk? I mean, or I don't know. It seems to me that if you have that kind of information, you have an obligation to come forward with it, because it's illegal. And they've been saying that. I mean, they've—you know, Wyden and Udall have been saying that this is illegal or that this is secret interpretation that the American public doesn't know about, and I think that they should come forward, because I—

WILLIAM BINNEY: Well, yeah, more importantly, it's a violation of

the constitutional rights of every American citizen. And that's a violation that they took an oath to defend against.

JACOB APPELBAUM: I think that it's—

AMY GOODMAN: Jacob Appelbaum?

JACOB APPELBAUM: You know, Cindy Cohn at the EFF is fighting the good fight.

AMY GOODMAN: Electronic Frontier Foundation?

JACOB APPELBAUM: Yeah, the Electronic Frontier Foundation is like the legal version of Riseup, in my mind, you know? They're really amazing. And they're fighting these cases, such as *NSA v. Jewel*. And I think that it is incredibly important basically to point out—and when we want to talk about Congress for a second, I mean, the judiciary has some—

AMY GOODMAN: We have 30 seconds.

JACOB APPELBAUM: They have some power, but what really—what really matters is that Congress needs to have people like Bill. They need to have people who actually understand the technology questioning people like General Alexander, not people who are bamboozled and fooled by the word "email" or the word "network." And that's what we need to do is we need to have people that know speak to the people that don't know. And that is Congress.

AMY GOODMAN: Jacob Appelbaum is a computer security researcher. He works with the TorProject.org. That's T-O-R Project-dot-org. William Binney directed the NSA's World Geopolitical and Military Analysis Reporting Group. That's the National Security Administration. He worked there for close to 40 years. And Laura Poitras is the Oscar-nominated filmmaker, her films, *My Country, My Country* and *The Oath*. This was part two of our broad discussion on the surveillance state. We began it on Friday. You can go to our website at democracynow.org to see the full discussion or read the transcript or listen.