State Surveillance

- 5-Part Special -

by **Amy Goodman**
April 2012
from DemocracyNow Website

Part 1

National Security Agency Whistleblower William Binney
...on Growing State Surveillance
April 20, 2012

In his first television interview since he resigned from the National Security Agency over its domestic surveillance program, **William Binney** discusses the NSA's massive power to spy on Americans and why the FBI raided his home after he became a whistleblower.

Binney was a key source for investigative journalist **James Bamford**'s recent exposé in Wired Magazine about how the NSA is quietly building the largest spy center in the country in Bluffdale, Utah.

The Utah spy center will contain near-bottomless databases to store all forms of communication collected by the agency, including private emails, cell phone calls, Google searches and other personal data.

Binney served in the NSA for over 30 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 that the NSA's data-mining program has become so vast that it could "create an Orwellian state."

Today marks the first time Binney has spoken on national television about NSA surveillance.

Video

Transcript

JUAN GONZALEZ: Today we bring you a Democracy Now! special on the growing domestic surveillance state and the Department of Homeland Security's efforts to spy on dissident journalists and activists. In a national broadcast exclusive, we're joined by 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 NSA is quietly building the largest spy center in the country in Bluffdale, Utah. The Utah spy center will contain nearly bottomless databases to store all forms of communication collected by the agency, including private emails, cell phone calls and Google searches and other personal data.

Binney served in the NSA for over 30 years, including a time as director of the NSA's World Geopolitical and Military Analysis Reporting Group. Since retiring from the NSA in 2001, he has warned that the agency's data-mining program has become so vast that it could, quote, "create an Orwellian state." Today marks the first time Binney has spoken on national television about surveillance by the National Security Agency.

AMY GOODMAN: We're also joined by two individuals who have been frequent targets of government surveillance: Laura Poitras, the Academy Award-nominated filmmaker, and Jacob Appelbaum, a computer security researcher who has volunteered with WikiLeaks. Poitras is the director of the documentary films My Country, My Country and The Oath. Both Poitras and Appelbaum have been repeatedly detained and interrogated by federal agents when entering the United States. Their laptops, cameras and cell phones have been seized, and presumably their data has been copied.

The Justice Department has also targeted Applebaum's online communications. In November, a federal judge ordered Twitter to hand over information about his account. In October, the Wall Street Journal revealed the Justice Department had obtained a secret court order to force Google and the internet provider Sonic.net to turn over information about Appelbaum's email accounts.

William Binney, Laura Poitras and Jacob Appelbaum will be speaking tonight at the Whitney Museum here in New York for a teach-in on surveillance. The three of them join us here in our studio together in a broadcast for the first time. We're going to begin with William Binney.

You worked for the National Security Agency for more than three decades.

WILLIAM BINNEY: Almost four.

AMY GOODMAN: Almost four decades.

WILLIAM BINNEY: Yeah.

AMY GOODMAN: You, for a time, directed the NSA's World Geopolitical and Military Analysis Reporting Group. Tell us what you did and then why you left and what happened to you afterwards.

WILLIAM BINNEY: Well, I was the technical director of that group, that basically looked at the world, so we looked at all the technical problems of - in the world, and see how we could solve collection, analysis and reporting on military and geopolitical issues all around the world, every country in the world. So, it was a rather large technical problem to tackle, but it - and one of the largest problems we thought we had was looking at the World Wide Web and all the ballooning and mushrooming communications in the world. And our ability to deal with that was diminishing over time, so I kind of referred to it as our inability to keep up with the rate of change. So, we were falling behind the rate of change.

So we - I had a very small group of people in a lab, and we decided to attack that problem. And we did it by looking at how we could graph the network of communications and all the communications in the world, and then - and then focus in on that graph and use the graph to limit what we wanted to attack. And we basically succeeded at that, but in the process, of course, we scooped up Americans from different places, so we had to protect their identities, according to our laws and privacy rights of U.S. citizens. So, under USSID 18, we built in protections to anonymize their identities, so you couldn't really tell who you were looking at.

JUAN GONZALEZ: And that's because the NSA could do surveillance from abroad, but not of U.S. citizens.

WILLIAM BINNEY: Well, and, you see, the World Wide Web routes things all over, so you never really know where U.S. citizens' communications are going to be routed. So, you - if you were collecting somewhere else on another continent, you could still get U.S. citizens. That's - see, that was a universal problem. So we devised how to do that and protect U.S. citizens. So - and this was all before 9/11. And we devised how to do that, made that effective and operating. So we were actually prepared to deploy about eight months before 9/11 and actually have a system that would run and manage the - what I call 20 terabytes a minute of activity.

So - but after 9/11, all the wraps came off for NSA, and they decided to - between the White House and NSA and CIA, they decided to eliminate the protections on U.S. citizens and collect on domestically. So they started collecting from a commercial - the one commercial company that I know of that participated provided over 300 - probably, on the average, about 320 million records of communication of a U.S. citizen to a U.S. citizen inside this country.

AMY GOODMAN: What company?

WILLIAM BINNEY: AT&T. It was long-distance communications. So they were providing billing data. At that point, I knew I could not stay, because it was a direct violation of the constitutional rights of everybody in the country. Plus it violated the pen register law and Stored Communications Act, the Electronic Privacy Act, the intelligence acts of 1947 and 1978. I mean, it was just this whole series of - plus all the laws covering federal communications governing telecoms. I mean, all those laws were being violated, including the Constitution. And that was a decision made that wasn't going to be reversed, so I could not stay there. I had to leave.

JUAN GONZALEZ: And I wanted to get back to, for a moment, when you say that you were developing a way to cope with the fact that the agency was falling behind, just because the sheer volume of the material that they were sweeping up was so great, that it was impossible, at times, to find the important intelligence material.

WILLIAM BINNEY: Yes.

JUAN GONZALEZ: So you, in essence, were creating a program that filtered out the valuable stuff.

WILLIAM BINNEY: Right. That's right.

JUAN GONZALEZ: What - did it have a name, the program?

WILLIAM BINNEY: Well, it was called Thin Thread. I mean, Thin Thread was our - a test program that we set up to do that. By the way, I viewed it as we never had enough data, OK? We never got enough. It was never enough for us to work at, because I looked at velocity, variety and volume as all positive things. Volume meant you got more about your target. Velocity meant you got it faster. Variety meant you got more aspects. These were all positive things. All we had to do was to devise a way to use and utilize all of those inputs and be able to make sense of them, which is what we did.

JUAN GONZALEZ: And when they didn't use your system, they - the NSA developed another or attempted to develop another system to do the same?

WILLIAM BINNEY: Well, that one failed. They didn't produce anything with that one.

AMY GOODMAN: And that one was called?

WILLIAM BINNEY: Trailblazer, yeah.

AMY GOODMAN: Trailblazer, and -

WILLIAM BINNEY: I called it - I called it five-year plan number one. Five-year plan number two was Turbulence. Five-year plan number three is -

AMY GOODMAN: And Trailblazer cost how much money?

WILLIAM BINNEY: That was, I think, in my - my sense, was a little over $4 billion.

AMY GOODMAN: Four billion dollars.

WILLIAM BINNEY: Right.

AMY GOODMAN: But it was scuttled. It was done away with in 2006?

WILLIAM BINNEY: Yes, '05, I think it was. But yes, that's right. And we developed our program with $3 million, roughly.

JUAN GONZALEZ: And Trailblazer was largely developed by SAIC, the -

WILLIAM BINNEY: Well, they were contributing contractors, yeah. But they - I think they had the lead - they were the lead contractors in some of contracts, yeah.

AMY GOODMAN: And why did they go with this one, though, ultimately, they did not use it? This is under Michael Hayden at the time?

WILLIAM BINNEY: Yes. Well -

AMY GOODMAN: Under the Bush administration?

WILLIAM BINNEY: Well, I thought - my sense was it was a good employment program. And it was a large budget program. It would spend money, a lot of money, so it would build the budget and -

AMY GOODMAN: Go to a major weapons manufacturer.

WILLIAM BINNEY: Right.

AMY GOODMAN: And heads of the agency, National Security Agency, would go back and forth working at NSA, working at SAIC.

WILLIAM BINNEY: It was - we called it an incestuous relationship, yeah.

AMY GOODMAN: What happened to you after you quit? You quit within a month of the 9/11 attacks.

WILLIAM BINNEY: Thirty-first of October of 2001, yeah.

AMY GOODMAN: And then what happened?

WILLIAM BINNEY: Well, we tried to form out the company to at least help the government to deal with some of the massive data problems they had, like in - even in the FBI, and also Customs and Border Protection and NRO and various other agencies. And every time we went somewhere to try to develop something, why, we got canceled, our contract got canceled, for - basically because, we have heard, anyway, that they were told that certain agencies didn't want them hiring us, so they didn't want us working for them, so...

JUAN GONZALEZ: And before you left, in that short period when it became obvious to you the direction that the NSA was going to, did you - when you raised objections or raised concerns, what was the response?

WILLIAM BINNEY: Well, I went directly to the Intelligence Committee, because it was their job to - because, first of all, when that happened, I mean, the people they had to use to set it up - since they used part of the program we developed to set it up, they had to use our people to set it up, initially, because no one else knew the code, and no one else knew how to get it operating. So, when they did that, they came - those people came to me and said, "You know, they're doing this," you know, and they told me what they were doing. And so I immediately went to the Intelligence Committee, because they were - the intelligence committees were formed to have oversight over the intelligence community to make sure they didn't monitor U.S. citizens. This was a fallout of the Church Committee back in the '70s. And the member of the staff that I went to went to Porter Goss, who was chairman of that committee at the time, and he referred her to General Hayden for any further. When it was the job of that committee to do the oversight on all this domestic spying, they weren't doing it, OK? Basically, the - at the time, according to Dick Cheney's interview on the 10th anniversary of 9/11, he said the - at that time, only the majority or minority leaders, the HPSCI and the SSCI, were involved in having knowledge about this program, Stellar Wind, which you had talked with Tom Drake about.

AMY GOODMAN: The former NSA -

WILLIAM BINNEY: Right, right.

AMY GOODMAN: - employee who was also a whistleblower.

WILLIAM BINNEY: And that was the program, of course, that Director Mueller reported was the

issue that - with the hospital visit with Ashcroft. So -

AMY GOODMAN: And explain that, very briefly, for - to remind people.

WILLIAM BINNEY: Well, the whole program, I guess, had to be reauthorized every 45 days, and they had to have the director of NSA, director of CIA and the attorney general sign an affidavit that they still needed the program and that it was legal. And when Comey and Goldsmith in the DOJ decided that this really was a violation of the Constitution and was illegal, then that issue came up. And that's what - that's what got everybody kind of disturbed and ready to - ready, actually, to resign in 2004, early 2004, I believe that was. And as a part of it was coming up for reauthorization, and so Gonzales left the White House, along with one other person I can't remember, and went to the hospital where Ashcroft was, because he was - had pancreatitis, I believe, and was in the hospital, and Comey was the acting attorney general. And so, at that point, they went to Ashcroft to see if he would overrule Comey, who had denied reauthorization and declared it basically illegal. And so, they tried to get Ashcroft to overrule that and went to the hospital to do that. And Director Mueller, I think, also quickly got to the hospital to help ensure that Ashcroft was not taken advantage of, I guess. So...

AMY GOODMAN: When was your home raided?

WILLIAM BINNEY: Twenty-sixth of July of 2007.

AMY GOODMAN: What happened? Where did you

WILLIAM BINNEY: I should - I should say that it was the morning of the second day after Gonzales's testimony, the then-Attorney General Gonzales's testimony, to the Senate Judiciary Committee on the TSP, the - what was called the TSP, which I refer to as a fabricated plan. It was created to cover a number of plans, one of which was Stellar Wind, and the others - which they didn't want to discuss. And the others were wiretapping.

And so, they picked on the wiretapping ones, because the public would generally say,

> "Yes, anybody that was potentially a terrorist, a foreign terrorist, communicating with anybody in the United States, we want you to monitor their communications."

So that was the acceptable part of it. But it was grouped with Stellar Wind and some other programs, so that they could give cover to it, talk about some programs, say they're talking about the Terrorist Surveillance Program, but it was basically a group of programs, some of which they did not want to talk about. And he did not testify to that at the - and I believe some of the - Whitehouse and Feingold, I think, were the two who were on the Senate Intelligence Committee that did challenge him at the time, saying he wasn't being truthful, and that was - he wasn't being completely honest. So...

AMY GOODMAN: You live where?

WILLIAM BINNEY: I live in Maryland, actually four miles from NSA.

AMY GOODMAN: And what happened?

WILLIAM BINNEY: They came busting in.

AMY GOODMAN: Who's "they"?

WILLIAM BINNEY: The FBI. About 12 of them, I think, 10 to 12. They came in with the guns drawn, on my house.

AMY GOODMAN: Where were you?

WILLIAM BINNEY: I was in the shower. I was taking a shower, so my son answered the door. And they of course pushed him out of the way at gunpoint and came running upstairs and found me in the shower, and came in and pointed the gun at me while I was, you know -

AMY GOODMAN: Pointed a gun at your head?

WILLIAM BINNEY: Oh, yeah. Yes. Wanted to make sure I saw it and that I was duly intimidated, I guess.

JUAN GONZALEZ: And what did they - what did they do at that point? Did they begin questioning you? Or they just took you to headquarters? Or -

WILLIAM BINNEY: No, no. Yeah, they basically separated us from - I was separated from my family. Took me on the back porch, and they started asking me questions about it. They were basically wanting me to tell them something that would implicate someone in a crime. And so, I told them that I didn't really know - they wanted to know about certain people, that was - they were the ones that were being raided at the same time, people who - we all signed - those who were raided that day, all of us signed the DOD-IG complaint. We were the ones who filed that complaint.

AMY GOODMAN: The Pentagon -

WILLIAM BINNEY: The Pentagon DOD-IG, against -

AMY GOODMAN: - inspector general complaint.

WILLIAM BINNEY: Against NSA, yes, talking about fraud - basically corruption, fraud, waste and abuse. And then -

AMY GOODMAN: Tom Drake was raided at the same time?

WILLIAM BINNEY: No, he was raided in November of that year. We were just the ones who signed it, were raided.

JUAN GONZALEZ: So, and who were the other people that were raided that same day?

WILLIAM BINNEY: Diane Roark, Kirk Wiebe and Ed Loomis.

AMY GOODMAN: Diane Roark worked for the Senate committee?

WILLIAM BINNEY: Diane was the senior staffer. She had the NSA account on the HPSCI side, on the House side. So she was monitoring. She was doing oversight. She was doing real oversight; the others weren't. Basically, the others were simply taking what the NSA said verbatim and taking them at their word. So, basically, that was not oversight. But Diane would probe and be prying into what they were saying to find out really clearly what was going on. And -

JUAN GONZALEZ: And ostensibly, they were searching for who was leaking information to the - who had leaked information to the New York Times.

WILLIAM BINNEY: That was the pretext, yes. But I accused them of being sent there by someone outside the FBI. And that - their body language told me that I hit it right on the head. So - and I also - after a while, they were questioning me, and I couldn't tell them anything, because I didn't know anything that would implicate any of the four of us, so -

AMY GOODMAN: They were looking for leaks.

WILLIAM BINNEY: Well, that was the pretext, the leak on the - to give the New York Times thing. The real thing - what they were really doing was retribution and intimidation so we didn't go to the Judiciary Committee in the Senate and tell them, "Well, here's what Gonzales didn't tell you, OK." That was what it was really all about. And also, it was retribution for that DOD-IG complaint, because it was a rather embarrassing report that they gave, so...

JUAN GONZALEZ: And what is it that Gonzales didn't tell them, in your perspective, in terms of what is happening to our national security surveillance situation?

WILLIAM BINNEY: Well, it was about - it was about Stellar Wind and all of the domestic spying.

AMY GOODMAN: We're going to break and come back to this conversation. William Binney was the technical director of the National Security Agency, which, by the way, is a number of times larger than the CIA, the National Security Agency's World Geopolitical and Military Analysis Reporting Group. When we come back, we'll also speak with a well-known hacker, Jacob Appelbaum, who has volunteered for WikiLeaks - he's a computer security researcher - and Laura Poitras, whose films, My Country, My Country and The Oath, are well known. She's been nominated for an Oscar.

This is Democracy Now! Back in a minute.

Part 2

Detained in The U.S.

- Filmmaker Laura Poitras Held and Questioned Some 40 Times at U.S. Airports -

April 20, 2012

The Academy Award-nominated filmmaker **Laura Poitras** discusses how she has been repeatedly detained and questioned by federal agents whenever she enters the United States.

Poitras said the interrogations began after she began working on her documentary, "My Country, My Country," about post-invasion Iraq. Her most recent film, "The Oath," was about Yemen and Guantánamo and follows the lives of two past associates of Osama bin Laden.

She estimates she has been detained approximately 40 times and has had her laptop, cell phone and personal belongings repeatedly searched. Tonight she is leading a surveillance teach-in at the Whitney Museum in New York City with our other guests, computer security researcher and government target Jacob Appelbaum and National Security Agency whistleblower William Binney.

Poiras is currently at work on a film about post-9/11 America.

Video

Transcript

AMY GOODMAN: Our guests are William Binney, who was technical director of the NSA's World Geopolitical and Military Analysis Reporting Group. He worked with the NSA for almost 40 years, National Security Agency. We're also joined by Laura Poitras, the Oscar-nominated filmmaker, and Jacob Appelbaum, a computer security researcher.

You two have something in common with each other. You - every time you come into the United States by plane, you are stopped, you are searched, you are interrogated. Laura Poitras, tell us about your experience. Your latest one?

LAURA POITRAS: Right. Well, I mean, I've been stopped at the border since 2006, since I started working on a series of films looking at U.S. post-9/11. And so, I've been - I've actually lost count of how many times I've been detained at the border, but it's, I think, around 40 times. And -

AMY GOODMAN: Four-zero.

LAURA POITRAS: Four-zero, right. And on this particular trip, lately they've been actually sending someone from the Department of Homeland Security to question me in the departing city, so I was questioned in London about what I was doing. I told them I was a journalist and that, you know, my work is protected, and I wasn't going to discuss it. And then, on this particular occasion, I landed at Newark Airport, and they - what they do when I'm flying, they do passport control inspection at the gate. So they make everyone who's deplaning show their passport. And so, that's how they -

JUAN GONZALEZ: So they don't even wait for you to get to Immigration.

LAURA POITRAS: No, I don't get - I don't get into Immigration. I get the escorted treatment from -

AMY GOODMAN: So they make everyone show the passport, until they get to you.

LAURA POITRAS: Right.

AMY GOODMAN: And then they take you off the plane.

LAURA POITRAS: And then they take me away. And then I'm escorted, first through Immigration. And so, this has been going on - you know, I've been through this several times and kind of know how it goes. But what happened on this particular trip, which was very disturbing, so -

AMY GOODMAN: Just a few weeks ago.

LAURA POITRAS: Yeah. So I was met by two agents at Newark. One of them is Agent Wassum. And I - when they met me, I took out my pen and paper to note their names and the time and - because I've always taken notes, so I have a record of the questions that I'm asked and how long I'm detained for, what's the focus of the interrogation, what they are doing to me. And on this occasion, I took out my pen, and I was ordered to put away my pen. And I didn't, and I continued to take notes. And I was ordered again to put away the pen, and I didn't. And then he threatened to handcuff me for not putting away my pen. And at that point, I put away my pen and then walked to Immigration and took out my pen again to take notes, was ordered again to put away my pen, and then was taken into secondary screening. And I asked to speak to a supervisor, explained I was a journalist, explained that legal counsel has told me that I should be taking notes of my detention and interrogation. And then I was told that I couldn't take notes, that I was free to take notes after I was finished being questioned. And then -

JUAN GONZALEZ: Under the theory that what? The pen was a weapon?

LAURA POITRAS: Oh, yeah, that's right. They said that my pen was a dangerous weapon. So that's what - that's Agent Wassum who said that, that my pen was a threat to them. And, you know, I mean, in terms of the context, you have to understand that I'm surrounded by border agents who are all carrying guns, and I'm taking out, you know, a pen that they find threatening. And so, this was, you know, profoundly upsetting. And then I was taken into - I was taken directly into an interrogation room and questioned. I took out my pen again. I was ordered by another agent to put it away. And this went on for quite some time. And I was told during this interrogation - I mean, I'm always asserting my rights as a journalist to not reveal my work, my sources.

AMY GOODMAN: You did a film on Yemen. You did a film on Iraq.

LAURA POITRAS: Yeah, yeah, yeah. And so, this detention started after I finished the first film in 2006, and which was about the occupation of Iraq. And I was told that I was refusing to cooperate with an investigation.

And then he said,

> "Well, it wasn't an investigation; it was questioning," but that I was refusing to cooperate.

And then I asserted my rights, that actually asserting one's rights is not refusing to cooperate.

And so, this went on for quite some time. And, I mean, it's something that's been happening for a while, and I've talked about it publicly, but also have been hesitant to, because I don't want to jeopardize the work that I do.

AMY GOODMAN: They took your computer? They took -

LAURA POITRAS: Not on this trip, no. In the past, yeah.

AMY GOODMAN: They've taken your computer?

LAURA POITRAS: On one occasion, they took my computer.

AMY GOODMAN: They've taken your phone?

LAURA POITRAS: Yeah. Yeah, on one occasion. I was actually - it was right after, a few days after they - it was actually maybe a week after Jacob's computer was detained.

AMY GOODMAN: Democracy Now! contacted the Department of Homeland Security for an explanation of why you were detained and interrogated at the airport on April 5th. We received a reply from Anthony Bucci, the public affairs specialist - that's B-U-C-C-I - in New York City for U.S. Customs and Borders Protection.

He emailed, quote:

> "Due to privacy laws, U.S. Customs and Border Protection is prohibited from discussing specific cases."

He went on to write, quote:

> "Our dual mission is to facilitate travel in the United States while we secure our borders, our people and our visitors from those that would do us harm like terrorists and terrorist weapons, criminals, and contraband."

He did not answer our additional questions.

LAURA POITRAS: Well, I guess they should add "journalist" to that list.

Part 3

"We Don't Live in a Free Country"

- Jacob Appelbaum on Being Target of Widespread Gov't Surveillance -

April 20, 2012

We speak with **Jacob Appelbaum**, a computer researcher who has faced a stream of interrogations and electronic surveillance since he volunteered with the whistleblowing website, WikiLeaks.

He describes being detained more than a dozen times at the airport and interrogated by federal agents who asked about his political views and confiscated his cell phone and laptop.

When asked why he cannot talk about what happened after he was questioned, Appelbaum says,

> "Because we don't live in a free country. And if I did, I guess I could tell you about it."

A federal judge ordered Twitter to hand over information about Appelbaum's account.

Meanwhile, he continues to work on the Tor Project, an anonymity network that ensures every person has the right to browse the internet without restriction and the right to speak freely.

Video

Transcript

JUAN GONZALEZ: Jacob, your experiences entering the United States at various times?

JACOB APPELBAUM: Well, after the summer of 2010, my life became a little hectic with regard to flying. I do a lot of traveling, working with the Tor Project. And after the summer of 2010, where I gave a speech at Hackers on Planet Earth in place of Julian Assange, I was targeted by the U.S. government and essentially, until the last four times that I've flown, I was detained basically every time. Sometimes men would meet me at the jetway, similarly, with guns.

AMY GOODMAN: Let us play that moment when you went to the HOPE conference.

JACOB APPELBAUM: Oh, dear.

AMY GOODMAN: Hackers on Planet Earth. Julian Assange was supposed to be there. He wasn't. You stood up. This is the beginning of what you said.

JACOB APPELBAUM: Hello to all my friends and fans in domestic and international surveillance. I'm here today because I believe that we can make a better world.

AMY GOODMAN: And what did you go on to say?

JACOB APPELBAUM: Basically, I went on to talk about how I feel that people like Bill need to come forward to talk about what the U.S. government is doing, so that we can make informed choices as a democracy. And I went on to talk about how WikiLeaks is a part of making that happen. And as long as we have excessive classification and secrecy, that we need a WikiLeaks, and we need to stand in solidarity together, so that people will have the information that they need to understand what's actually happening in their names.

JUAN GONZALEZ: You mentioned the Tor Project that you work with. What is it?

JACOB APPELBAUM: The Tor Project is an anonymity network, which ensures that each person has the right to read, without restriction, and the right to speak freely, with no exception.

AMY GOODMAN: T-O-R?

JACOB APPELBAUM: TorProject.org. And the basic idea is that every person in the world has the right to read and the right to speak freely. And using their software, using principles of mutual aid and solidarity - something familiar to Democracy Now! viewers, I imagine - it's possible for everybody to use this anonymity network, spread out across the planet. It's a thing that's useful for resisting so-called lawful interception. So, for example, when Mubarak in Egypt wants to wiretap someone, they only see an activist talking to the Tor network; they don't see that person connecting to Twitter. And that is something that can be used by everybody everywhere to resist so-called lawful interception.

JUAN GONZALEZ: And you use a program that was actually developed by the U.S. government?

JACOB APPELBAUM: Well, yeah. So, originally, the Tor Project is born from ideas that come from the anonymity community, of which the U.S. military has actually contributed quite heavily to. But since the times of the original onion routing patents, it has become a free software project, where, as far as I know, the U.S. Navy has contributed zero lines of code to it, but certainly lots of good ideas, because they understand, as many other people do, that if everyone has anonymous communication, that means everyone does, and if only special people do, it means that you can tell that those are special people that have special privileges, and you can basically see who they are.

So, for example, the Riseup Collective, which you mentioned earlier on the show, they run a number of tor nodes. And I run some, and many other people do. And as long as you get one good one, you have some of the properties that you need. And this helps people to resist not just so-called lawful interception, but also to resist censorship. So if you can't see inside of the communications, you can't selectively discriminate based on the content.

AMY GOODMAN: Just to say that in our news headlines today, we said the FBI has just seized a computer server at the New York facility shared by the internet organization Riseup Networks and May First/People Link. But I want to go back to your experience at the airport. If you could just briefly say - I mean, it's been dozens and dozens of times that you have -

JACOB APPELBAUM: I don't fly as much as Laura, and Laura has been at it for a lot longer than I have. But in the period of time since they've started detaining me, around a dozen-plus times. I've been detained a number of times. The first time I was actually detained by the Immigration and Customs Enforcement, I was put into a special room, where they frisked me, put me up against the wall. One guy cupped me in a particularly uncomfortable way. Another one held my wrists. They took my cell phones. I'm not really actually able to talk about what happened to those next.

AMY GOODMAN: Why?

JACOB APPELBAUM: Because we don't live in a free country. And if I did, I guess I could tell you about it, right? And they took my laptop, but they gave it back. They were a little surprised it didn't have a hard drive. I guess that threw them for a loop. And, you know, then they interrogated me, denied me access to a lawyer. And when they did the interrogation, they has a member of the U.S. Army, on American soil. And they refused to let me go. They tried - you know, they tried their usual scare tactics. So they sort of implied that if I didn't make a deal with them, that I'd be sexually assaulted in prison, you know, which is the thing that they do these days as a method of punitive punishment, and they of course suggested that would happen.

AMY GOODMAN: How did they imply this?

JACOB APPELBAUM: Well, you know, they say, "You know, computer hackers like to think they're all tough. But really, when it comes down to it, you don't look like you're going to do so good in prison." You know, that kind of stuff.

JUAN GONZALEZ: And what was the main thrust of the questions they were asking you?

JACOB APPELBAUM: Well, they wanted to know about my political views. They wanted to know about my work in any capacity as a journalist, actually, the notion that I could be in some way associated with Julian. They wanted, basically, to know any -

AMY GOODMAN: Julian Assange.

JACOB APPELBAUM: Julian Assange, the one and only. And they wanted - they wanted, essentially, to ask me questions about the Iraq war, the Afghan war, what I thought politically. They didn't ask me anything about terrorism. They didn't ask me anything about smuggling or drugs or any of the customs things that you would expect customs to be doing. They didn't ask me if I had anything to declare about taxes, for example, or about importing things. They did it purely for political reasons and to intimidate me, denied me a lawyer. They gave me water, but refused me a bathroom, to give you an idea about what they were doing.

AMY GOODMAN: What happened to your Twitter account?

JACOB APPELBAUM: Well, the U.S. government, as I learned while I was in Iceland, actually, sent what's called an administrative subpoena, or a 2703(d) order. And this is, essentially, less than a search warrant, and it asserts that you can get just the metadata and that the third party really doesn't have a standing to challenge it, although in our case we were very lucky, in that we got to have - Twitter actually did challenge it, which was really wonderful. And we have been fighting this in court.

And without going into too much detail about the current court proceedings, we lost a stay recently, which says that Twitter has to give the data to the government. Twitter did, as I understand it, produce that data, I was told. And that metadata actually paints - you know, metadata and aggregate is content, and it paints a picture. So that's all the IP addresses I logged in from.

It's all of the, you know, communications that are about my communications, which is Bill's specialty, and he can, I'm sure, talk about how dangerous that metadata is.

Part 4

Whistleblower:
The NSA is Lying-U.S. Government Has Copies of Most of Your Emails

April 20, 2012

National Security Agency whistleblower **William Binney** reveals he believes domestic surveillance has become more expansive under President Obama than President George W. Bush.

He estimates the NSA has assembled 20 trillion "transactions" - phone calls, emails and other forms of data - from Americans. This likely includes copies of almost all of the emails sent and received from most people living in the United States.

Binney talks about Section 215 of the USA PATRIOT Act and challenges NSA Director Keith Alexander's assertion that the NSA is not intercepting information about U.S. citizens.

Video

Transcript

JUAN GONZALEZ: Well, I wanted to ask William Binney about this issue. When it comes to snail mail, the old postal system, it's very tough for the government to intercept mail, except in times of war, particular situations. When it comes to phone conversations, land phone conversations, you need a warrant to be able to intercept phone conversations. But what about email, and what about

the communication now that is really the dominant form that not only Americans, but many people around the world communicate? What are the restrictions on the government in terms of email?

WILLIAM BINNEY: Well, after some of the laws they passed, like the PATRIOT Act and their secret interpretation of Section 215, which is - my view, of course, is same as Tom Drake's, is that that gives them license to take all the commercially held data about us, which is exceedingly dangerous, because if you take that and put it into forms of graphing, which is building relationships or social networks for everybody, and then you watch it over time, you can build up knowledge about everyone in the country. And having that knowledge then allows them the ability to concoct all kinds of charges, if they want to target you. Like in my case, they fabricated several charges and attempted to indict us on them. Fortunately, we were able to produce evidence that would make them look very silly in court, so they didn't do it. In fact, it was - I was basically assembling evidence of malicious prosecution, which was a countercharge to them. So...

AMY GOODMAN: Do you believe all emails, the government has copies of, in the United States?

WILLIAM BINNEY: I would think - I believe they have most of them, yes.

AMY GOODMAN: And you're speaking from a position where you would know, considering your position in the National Security Agency.

WILLIAM BINNEY: Right. All they would have to do is put various Narus devices at various points along the network, at choke points or convergent points, where the network converges, and they could basically take down and have copies of most everything on the network.

AMY GOODMAN: Jacob, your email?

JACOB APPELBAUM: Well, I selectively chose to use certain public services, like Sonic.net and Gmail, and I specifically did that so as to serve as a warning to other people. I didn't use it for anything interesting, never once emailed Julian, for example, from those accounts. But the U.S. government again asserted in those cases, according to the Wall Street Journal, which is one way to find out about what's going on with you - they asserted that they have the right to all that metadata. And it is possible - on Monday, I had a little interaction with the FBI, where they sort of hinted that maybe there might be a national security letter for one of my email accounts, which is also hosted by Google, specifically because I want to serve as a canary in a coal mine for other people.

AMY GOODMAN: A national security letter - it's believed the government has given out hundreds of thousands of those.

JACOB APPELBAUM: Yeah.

AMY GOODMAN: I have also written about NSLs. But if you get one, you are not allowed to talk about it, on pain of something like up to five years in prison, even to mention that you were handed a national security letter that said turn something over.

JACOB APPELBAUM: Yeah. That was the case of Nick Merrill, for example, who's a brave American, who essentially fought and won the NSL that was handed down to him.

AMY GOODMAN: And the librarians of Connecticut -

JACOB APPELBAUM: Yes.

AMY GOODMAN: - who were taking on the USA PATRIOT Act and didn't want to give information over about patrons in the library that the FBI wanted to get information on.

JACOB APPELBAUM: Right, absolutely. So, an NSL, what's specifically scary about it is that all that is required is for an FBI agent to assert that they need one, and that's it. And you don't have a chance to have judicial review, because you aren't the one served. Your service provider will be served. And they can't tell you, so you don't get your day in court.

AMY GOODMAN: Laura, can you set up this clip that we have?

LAURA POITRAS: Yes, actually, this is what Jake was alluding to. On Monday, there was a panel at the Open Society Institute. And Jake - and there was a deputy general counsel of the FBI who was present, and Jake had the opportunity to question her about national security letters.

JACOB APPELBAUM: Are you including national security letters in your comment about believing that there is judicial oversight with the FBI's actions?

FBI DEPUTY GENERAL COUNSEL: National security letters and administrative subpoenas have the ability to have judicial oversight, yes.

JACOB APPELBAUM: How many of those actually do have judicial oversight, in percentage?

FBI DEPUTY GENERAL COUNSEL: What do you mean by that? How many have -

JACOB APPELBAUM: I mean, every time you get a national security letter, you have to go to a judge? Or -

FBI DEPUTY GENERAL COUNSEL: No, as you well know, national security letters, just like administrative subpoenas, you don't have to go to a judge. The statute does allow for the person on whom those are served to seek judicial review. And people have done so.

JACOB APPELBAUM: And in the case of the third parties, such as, say, the 2703(d) orders that were served on my - according to the Wall Street Journal - my Gmail account, my Twitter account, and my internet service provider account, the third parties were prohibited from telling me about it, so how am I supposed to go to a judge, if the third party is gagged from telling me that I'm targeted by you?

FBI DEPUTY GENERAL COUNSEL: There are times when we have to have those things in place. So, at some point, obviously, you became aware. So at some point, the person does become aware. But yes, the statute does allow us to do that. The statute allows us.

AMY GOODMAN: Now, Jacob, explain who she was again.

JACOB APPELBAUM: So, my understanding is that she's the deputy general counsel of the FBI.

AMY GOODMAN: And the significance of what she has just said?

JACOB APPELBAUM: Essentially, what she says is,

> "We are just and righteous because you get judicial review. But there are some cases where you don't, and we are still just and righteous. And you should trust us, because COINTELPRO will never happen again."

That's what I heard from that. And, in fact, later, someone asked about COINTELPRO and said, "How can we" -

AMY GOODMAN: The counterintelligence program that targeted so many dissidents in the 1970s.

JACOB APPELBAUM: Yeah. Tried to get Martin Luther King Jr. to kill himself, for example. The FBI wrote him a letter and encouraged him to commit suicide. So for her to suggest that it is just and right and that we should always trust them sort of overlooks the historical problems with doing exactly that for any people in a position of power, with no judicial oversight.

JUAN GONZALEZ: William Binney, what about the companies that are approached by the government to participate or facilitate the surveillance? Your sense of the degree of opposition that they're mounting, if at all? And also, has there been any kind of qualitative change since the Obama administration came in versus what the Bush administration was practicing?

WILLIAM BINNEY: Well, first of all, I don't think any of them opposed it in any way. I mean, they were approached to saying, "You'll be patriotic if you support us." So I think they saluted and said, "Yes, sir," and supported them, because they were told it was legal, too. And then, of course, they had to be given retroactive immunity for the crimes they were committing. So -

JUAN GONZALEZ: Approved by President Obama.

WILLIAM BINNEY: And President Bush, yeah. It started with Bush, yeah.

JUAN GONZALEZ: And the differences in the administrations?

WILLIAM BINNEY: Actually, I think the surveillance has increased. In fact, I would suggest that they've assembled on the order of 20 trillion transactions about U.S. citizens with other U.S. citizens.

AMY GOODMAN: How many?

WILLIAM BINNEY: Twenty trillion.

AMY GOODMAN: And you're saying that this surveillance has increased? Not only the -

WILLIAM BINNEY: Yes.

AMY GOODMAN: - targeting of whistleblowers, like your colleagues, like people like Tom Drake, who are actually indicted under the Obama administration -

WILLIAM BINNEY: Right.

AMY GOODMAN: - more times - the number of people who have been indicted are more than all presidents combined in the past.

WILLIAM BINNEY: Right. And I think it's to silence what's going on. But the point is, the data that's being assembled is about everybody. And from that data, then they can target anyone they want.

AMY GOODMAN: Bill Binney, talk about Bluffdale, Utah. What is being built there?

WILLIAM BINNEY: Well, a very large storage device, basically, for remote interrogation and remote processing. That's the way I view that. Because there's not enough people there to actually work the data there, so it's being worked somewhere else.

AMY GOODMAN: Where do you get the number 20 trillion?

WILLIAM BINNEY: Just by the numbers of telecoms, it appears to me, from the questions that CNET posed to them in 2006, and they published the names and how - what the responses were. I looked at that and said that anybody that equivocated was participating, and then estimated from that the numbers of transactions. That, by the way, estimate only was involving phone calls and emails. It didn't involve any queries on the net or any assembles - other - any financial transactions or credit card stuff, if they're assembling that. I do not know that, OK.

JUAN GONZALEZ: And the original - the original allegations that you made, in terms of the crimes being committed under the Bush administration in terms of the rights of American citizens, could you detail those?

WILLIAM BINNEY: Well, I made that - I reported the crime when I was raided in 2007. And it was that Bush and Cheney and Hayden and Tenet conspired to subvert the Constitution and violate various laws of the - that exist in the statute at the time, and here's how they did it. And I was reporting this to the FBI on my back porch during the raid. And I went through Stellar Wind and told them what it did and what the information it was using and how they were spying on - or assembling data to be able to spy on any American.

AMY GOODMAN: I want to go to a clip of Congress Member Hank Johnson - he's the Georgia Democrat - questioning National Security Administration director, General Keith Alexander, last month, asking him whether the NSA spies on U.S. citizens.

> REP. HANK JOHNSON: Does the NSA routinely intercept American citizens' emails?
>
> GEN. KEITH ALEXANDER: No.
>
> REP. HANK JOHNSON: Does the NSA intercept Americans' cell phone conversations?
>
> GEN. KEITH ALEXANDER: No.
>
> REP. HANK JOHNSON: Google searches?
>
> GEN. KEITH ALEXANDER: No.
>
> REP. HANK JOHNSON: Text messages?
>
> GEN. KEITH ALEXANDER: No.
>
> REP. HANK JOHNSON: Amazon.com orders?
>
> GEN. KEITH ALEXANDER: No.
>
> REP. HANK JOHNSON: Bank records?

GEN. KEITH ALEXANDER: No.

REP. HANK JOHNSON: What judicial consent is required for NSA to intercept communications and information involving American citizens?

GEN. KEITH ALEXANDER: Within the United States, that would be the FBI lead. If it was a foreign actor in the United States, the FBI would still have the lead and could work that with NSA or other intelligence agencies, as authorized. But to conduct that kind of collection in the United States, it would have to go through a court order, and the court would have to authorize it. We are not authorized to do it, nor do we do it.

AMY GOODMAN: That was General Keith Alexander, the NSA director, being questioned by Democratic Congress Member Hank Johnson. Bill Binney, he's the head of your agency, of the NSA. Explain what he's saying - what he's not saying, as well.

WILLIAM BINNEY: Well, I think it's - part of it is a term, how you use the term "intercept," as to whether or not what they're saying is, "We aren't actually looking at it, but we have it," you know, or whether or not they're actually collecting it and storing it somewhere.

JUAN GONZALEZ: So the mistake of the congressman was not to ask, "Are you collecting information?"

WILLIAM BINNEY: Well, he also said things like, "We don't collect" - or, "We don't collect against U.S. citizens unless we have a warrant." And then, at the same time, he said that we don't - at the same interview, he said, "We don't have the capability to collect inside this country." Well, those are kind of contradictory.

AMY GOODMAN: Is he lying? Is General Keith Alexander lying?

WILLIAM BINNEY: I wouldn't - you know, the point is how you split the words. I wouldn't say "lying." It's a kind of avoiding the issue.

AMY GOODMAN: Jacob Appelbaum, how does this relate to you? And how powerful is General Keith Alexander?

JACOB APPELBAUM: I was saying to Bill that I think he's probably the most powerful person in the world, in the sense that -

AMY GOODMAN: More powerful than President Obama?

JACOB APPELBAUM: Well, sure. I mean, if he controls the information that arrives on Obama's desk, and Obama makes decisions based on the things on his desk, what decisions can he make, if - except the decisions presented to him by the people he trusts? And when the people he trusts are the military, the military makes the decisions, then the civilian government is not actually in power.

AMY GOODMAN: Bill Binney, you're nodding your head.

WILLIAM BINNEY: Yes. I mean, well, for example, their responsibility is to interpret what they have and report up echelon. So, I mean, that's the responsibility of all the intelligence agencies. So, they basically filter the information to what they believe is important, which is what they should do, because, you know, they're occupying - it takes time for leaders to review material to make decisions. So they have to boil it down as best they can. So it's a function of their processing, but it is important that they do it correctly to make sure the information that gets there is correct and complete as it can.

AMY GOODMAN: Is General Alexander more powerful than President Obama?

WILLIAM BINNEY: In the sense of making - of presenting information for decision making, sure.

JUAN GONZALEZ: And Laura, the impact on journalists, who have to go through what you go - you've gone through the last few years, just to be able to report what's going on with our government? The chilling effect that this has on - maybe not on you, but on many other journalists?

LAURA POITRAS: Sure. I mean, I feel like I can't talk about the work that I do in my home, in my place of work, on my telephone, and sometimes in my country. So the chilling effect is huge. It's enormous.

AMY GOODMAN: You keep your computers and telephones away from conversations you're having in a room?

LAURA POITRAS: Yeah. When we had a meeting with you, remember, we told you - we kicked all your cell phones and all your computers out of the room.

AMY GOODMAN: You un - the wired phone, you unwired.

LAURA POITRAS: Yeah.

AMY GOODMAN: My cell phone, you didn't allow me to have it in the room. And you made sure there were no computers in the room.

LAURA POITRAS: Right.

AMY GOODMAN: Why?

LAURA POITRAS: Because we wanted - well, we wanted to talk about - because we were bringing - we were bringing William to New York. And -

AMY GOODMAN: We have to leave it there, but we're going to go online right now at democracynow.org. We're going to continue this conversation with Bill Binney of the NSA, formerly with NSA; Laura Poitras and Jacob Appelbaum.

Part 5

More Secrets on Growing State Surveillance
- Exclusive with NSA Whistleblower and Targeted Hacker -

April 23, 2012

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**
- 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.

Video

Rush Transcript

-

AMY GOODMAN: We turn to part two of Democracy Now!’s whistleblowerwilliam">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, cell phones 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 cell phones 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.

Return to The NSA - The Super Secret National Security Agency