Display full version

FRIDAY, APRIL 20, 2012

"We Don't Live in a Free Country": Jacob Appelbaum on Being Target of Widespread Gov't Surveillance

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 cellphone 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. *This interview is part of a 5-part special on growing state surveillance. Click here to see segment 1, 2, 4 and 5*state. [includes rush transcript]

TRANSCRIPT

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

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 cellphones. 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.

This interview is part of a 4-part special. Click here to see segment 1, 2, and 4.