



TUNE IN TO THE
SOUND OF DEMOCRACY

Justice Talking Radio Transcript

Domestic Spying: What are the Checks on Presidential Power? – Air Date: 2/6/2006

After recent reports in the New York Times, the Bush Administration has admitted it authorized the National Security Agency to eavesdrop on suspected terrorists within the United States without obtaining court approval. These actions raise significant questions about how far government can go to track terrorists and whether our civil liberties are on a crash course with executive power. Join us for this edition of Justice Talking as we take a look at U.S. intelligence policies and ask whether they are legal and effective at safeguarding the homeland.

This transcript is being provided free of charge for educational purposes. The views expressed herein are those solely of the guests and do not reflect those of the Annenberg Public Policy Center or NPR. Although every effort is made to make a verbatim rendering of the program, this transcript may vary slightly from the audio version and may contain minor grammatical or spelling errors. For permission to reprint, please contact Laura Sider at the University of Pennsylvania's Annenberg Public Policy Center, (215) 573-8919.

MARGOT ADLER: From NPR, this is Justice Talking. I'm Margot Adler. On today's show, domestic spying. Should there be checks on presidential power? After recent reports in the New York Times, the Bush Administration has admitted it authorized the National Security Agency to eavesdrop on suspected terrorists within the United States without obtaining court approval. These actions raise significant questions about how far government can go to track terrorists and whether our civil liberties are on a crash course with executive power. Stay with us as we take a look at U.S. intelligence policies and ask whether they are legal and effective at safeguarding our country.

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. The National Security Agency, or NSA, isn't part of the government that you usually hear about. That is until recently. The revelation by the New York Times that President Bush authorized the NSA to implement a domestic surveillance government has created quite a stir. Arguments over presidential power and what rules should govern intelligence gathering have reached new

heights. The President has been working hard to defend his position. Here he is in his recent State of the Union speech.

PRESIDENT BUSH: It is said that prior to the attacks of September the 11th, our government failed to connect the dots of the conspiracy. We now know that two of the hijackers in the United States placed telephone calls to Al Qaeda operatives overseas. But we did not know about their plans until it was too late. So to prevent another attack, based on the authority given to me by the Constitution, by statute, I have authorized a terrorist surveillance program to aggressively pursue the international communications of suspected Al Qaeda operatives and affiliates to and from America.

MARGOT ADLER: The issues at hand are complex and numerous. And in this hour of Justice Talking, we hope to clear up some of the questions you may have. Later on in the show, we'll hear a debate between a law professor who believes the President has overstepped his authority and a former White House attorney who says the President is on solid legal footing. And if you've ever wondered just how surveillance works, stick around. You'll find out about how your phone calls and emails and could be intercepted.

UNIDENTIFIED MALE: One interesting little tidbit is that if you look around the country at the ground stations that are used to convey satellite communications in and out of the United States, often with 60 or 70 miles of a ground station, there is also a secret NSA base.

MARGOT ADLER: But first, Eric Lichtblau joins me. He is the Justice Department correspondent at the New York Times. He and James Risen broke the story about the Bush administration's use of domestic surveillance. Welcome, Eric.

ERIC LICHTBLAU: Thanks for having me.

MARGOT ADLER: You wrote a story in the New York Times that was printed in December that said the President had authorized the National Security Administration, the NSA, to conduct domestic surveillance on U.S. citizens. What was the NSA asked to do?

ERIC LICHTBLAU: Well, in the months after 9/11, there was a major rethinking of the role of the National Security Agency, which traditionally and legally has been confined to overseas foreign signals intelligence. What President Bush did was to authorize by secret executive order the NSA's interception of some emails and phone calls within the United States so long as one party was outside the United States. And the key element of this was that these interceptions did not require warrants which traditionally would have been granted by a court set up in 1978, known as the Foreign Intelligence Surveillance Act Court.

MARGOT ADLER: Now, was the timeline for this after 9/11? I've heard some conflicting stories that the NSA might have even begun spying before.

ERIC LICHTBLAU: There's no indication that this eavesdropping program began before 9/11. There's some confusion and uncertainty as to exactly how soon after 9/11 this started. What we've reported is that a sort of mini version of this program began almost immediately after 9/11, involving calls, emails and communications out of and into Afghanistan from the United States. It was some point after that (the White House has still not made clear exactly when President Bush first signed the executive order—it appears to have been early 2002 or perhaps late 2001) that this program was formalized and broadened beyond Afghanistan to include any and all international communications beyond Afghanistan.

MARGOT ADLER: Now, the NSA program doesn't simply wiretap individuals as I understand it. It vacuums up huge amounts of data and looks for patterns. How does that work?

ERIC LICHTBLAU: Well, what we've reported is that the NSA now has access to enormous telecommunication switches, mostly on the East Coast, that bring in everything into and out of the United States from overseas. And by virtue of this access to those switches by a voluntary agreement with some of the biggest telecom companies in the country, the NSA is able to look for patterns in terms of phone calls, when and where people are being called, when and where emails are being sent, from what country, what time of day, things like that.

Now, the President and General Michael Haden, who was the point man on this program, draw a distinction between that broader program, which is in effect data mining, and the specific eavesdropping program that you're referring to. And to be honest, the relationship between the broader data mining and the targeted eavesdropping which we've reported involves as many as 500 people and phone numbers and email addresses at any one time, and thousands over the last four years, but the relationship between the broader data mining and those targeted eavesdropping is still a subject of some debate.

MARGOT ADLER: And I would wonder if there are legal differences, in fact, between what's allowed if you're talking about data mining and specific eavesdropping on specific conversations.

ERIC LICHTBLAU: Well, I think there are. And I think that's a good point. The area of the law as far as data mining is very, very grey. There are no really clear-cut statutes as to what is allowed. There are certain materials—Social Security numbers, IRS records and things like that—that are very restricted in their use. But the whole area of what could or could not be gained from data mining is really an evolving area. The law seems to be clearer on the subject of these actual eavesdropping operations.

The President has, of course, argued that he has the inherent constitutional authority to do what he did, but here have been any number of legal critics, a lot of politicians, both Democratic and Republican, who take issue with that. And there was a report from the Congressional Research Service, which is an independent non-partisan research arm of Congress, which challenged virtually all of the key legal points that the White House made in defending the legality of the program, particularly the idea which President Bush and

others have cited repeatedly, that Congress gave him this authority in the days after 9/11 when it authorized him to use all necessary and appropriate force against those responsible for 9/11. The White House has said many times that that was the authorization they needed and that this operation, which they refer to as “Signals Intelligence,” is a key part of the warfare. Most members of Congress have said this was not what they intended when they allowed Bush the military authority to go into Afghanistan days after 9/11, and the Congressional Research Service agreed that there were major legal problems with the legal rationalization.

MARGOT ADLER: Let’s talk a little bit about FISA. The administration says it needs this power to eavesdrop on citizens, that the existing judicial checks on executive power don’t allow for the kind of agility and flexibility that the government needs. But one of the things that I read was that between 1995 and 2004 there were more than 10,000 FISA requests and only four were rejected. And since electronic surveillance can begin 72 hours before requesting permission, I’m wondering if the administration’s argument makes sense. And why did the administration feel that it needed this? Did it simply want to assert presidential authority? Or was there something more?

ERIC LICHTBLAU: The White House has been asked this repeatedly and they cite the reasons that you cite, that the FISA system in their view is not agile and flexible enough. When pressed for details as to whether there have been cases in which they have not been able to get a warrant quickly enough to eavesdrop on an Al Qaeda suspect, they have not provided any details to be honest.

MARGOT ADLER: Recently, FISA judges from around the country went to Washington to get briefed on the administration’s use of surveillance. What can you tell us about that meeting? Weren’t many of those judges unaware of what the administration was doing?

ERIC LICHTBLAU: Right. What we reported in our initial story was that on the current court, only the presiding judge, Judge Kollar-Kotelly, had been briefed on this program. And that she herself had raised some concerns, particularly in 2004, about the program and the way it appears to have been used in order to generate traditional FISA warrants. What we reported was that there were some cases in which information growing out of this warrantless program appeared to have been used in order to go back to the court and say, well now we have information establishing probable cause on this person. She was concerned about that process and essentially walled off information from this extraordinary program. As far as we know, no other judges on the FISA court, aside from her as presiding judge, were aware of the existence of the program at the time. And when our story ran on December 16th, almost immediately one of the judges, one of the eleven judges who sit on the court, Judge Robertson, resigned from the FISA court in protest.

MARGOT ADLER: You reported this story a year ago, yet the New York Times didn’t publish it after the administration asked it not to. And around every coffee klatch and water cooler that I’ve been around has been all this speculation as to why the New York Times decided not to publish it? I have no idea if you have any way of enlightening us on any of that.

ERIC LICHTBLAU: What the paper said in our original story was that we did hold the story for a year at the request of the administration and we conducted additional reporting. You know, the concerns that we were hearing earlier became even more evident, about some of the legal and operational issues, and the paper decided to move ahead with the story which I'm glad they did.

MARGOT ADLER: There's a possibility that you might be subpoenaed by the Justice Department and forced to reveal your sources in the spying story. What do you think will happen? And what do you plan to do if you're subpoenaed?

ERIC LICHTBLAU: I certainly hope it doesn't come to that. And for reasons that I probably can't get into, I don't think it will come to that. But as my colleague on the story, Jim Risen, has said in the past, I think the people that came to us were whistleblowers in the true sense. I would never give up a source, especially in this extraordinary situation, and I know Jim wouldn't either. I know there have been any number of comments from politicians on both sides of the aisle who suggest that perhaps equal time should be devoted to investigation into the program and some of the questions about it rather than a leak investigation.

MARGOT ADLER: Thank you so much, Eric.

ERIC LICHTBLAU: Thanks for having me.

MARGOT ADLER: Eric Lichtblau is the Justice Department correspondent for the New York Times. He and one of his colleagues broke the story about how the Bush Administration used domestic surveillance without first obtaining warrants. He is currently working on a book about the Justice Department in the Bush Administration. To learn more about domestic spying and presidential powers, check out our website, justicetalking.org.

MARGOT ADLER: Coming up on Justice Talking, two lawyers square off over whether the President broke the law when he approved the NSA's domestic surveillance program. And we'll also hear from an attorney who suspects she and her clients have been spied on.

UNIDENTIFIED FEMALE: I would be frankly astounded if our communications weren't being intercepted.

MARGOT ADLER: All this and more. Don't go away.

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. For the past several weeks, the Bush administration has been vigorously defending its policy of domestic spying by the National Security Agency. President Bush argues that he is using every legal means to

protect the country from terrorist attack. But as Reese Erlich reports, some critics say the NSA policy is just one part of a much wider pattern of illegal domestic spying.

REESE ERLICH: Back in June of 2004, antiwar activist Scott Parkin helped organize a protest at Halliburton's Houston headquarters. It took place as the U.S. handed over formal power to an Iraqi regime.

SCOTT PARKIN: We had an Iraqi independence day where they were handing over their independence to Halliburton. We had a table where we served peanut butter and jelly sandwiches and drinks. The theme of it was cook food, not books.

REESE ERLICH: Only about eight people showed up for the demonstration and Parkin didn't think more about it. Then last month, Newsweek magazine uncovered government documents indicating that the innocuous protest in Houston was monitored by a secret Pentagon agency. Parkin suspects his emails and phone calls are monitored by the NSA as well. Last year, he visited Australia and encouraged antiwar protests. As a result, he was deported.

SCOTT PARKIN: I had to call Australia quite a bit. And so it wouldn't surprise me at all that the NSA was monitoring me. I'm relatively sure that the Australian authorities are monitoring my communications between here and Australia.

REESE ERLICH: Parkin can't prove that the NSA is listening to his calls. That's top secret information. The ACLU has filed a lawsuit on behalf of other people to stop the government from illegally monitoring domestic calls. Ann Beeson, lead attorney in that case, says illegal domestic spying has increased dramatically under the Bush administration.

ANN BEESON: The kind of spying that we are seeing now, whether it's through the National Security Agency, through presence at public rallies, through infiltration of peaceful protest groups, all of those techniques look not just similar, but practically identical to the techniques that were used during the '50s and '60s and '70s during the J. Edgar Hoover era of the FBI.

REESE ERLICH: In a January speech at Kansas State University, President Bush said he respects civil liberties and is not conducting illegal surveillance. He argues that the government narrowly focuses on intercepting important information that could stop terrorist attacks.

PRESIDENT BUSH: I repeat to you, you know, you hear words domestic spying. These are not phone calls within the United States. It's a phone call of an Al Qaeda...a known Al Qaeda suspect making a phone call into the United States. I'm mindful of your civil liberties. And so I had all kinds of lawyers review the process.

REESE ERLICH: But critics such as the ACLU cite a recent New York Times article in which agents from various investigative agencies complained that the NSA program goes well beyond suspected Al Qaeda subjects and gave them hundreds of useless leads.

ANN BEESON: There is no evidence at all that would suggest that it had been remotely effective in fighting against terrorism. And in fact, you have now high level officials inside the FBI saying that most of the data that they got from the National Security Agency was absolutely useless and was a waste of valuable resources that could have been used to go after the real terrorists.

REESE ERLICH: Attorney General Alberto Gonzalez strongly disagrees. In a speech at the Georgetown Law School, he said the program has been successful and necessary because existing surveillance laws don't adequately protect the public. He said the Federal Intelligence Security Act, or FISA, which grant the President the right to tap phones for 72 hours without court approval isn't enough.

ATTORNEY GENERAL GONZALEZ: The optimal way to achieve the necessary speed and agility is to leave the decisions about particular intercepts to the judgment of professional intelligence officers. They can make that call quickly.

ANN BEESON: Under our system of democracy, it was not up to President Bush to decide whether or not existing laws were adequate.

REESE ERLICH: ACLU attorney Ann Beeson argues that Congress passed the FISA law in 1978 to limit presidential wiretapping authority even during war time.

ANN BEESON: If he had needed additional laws at the very least, he should have gone to Congress and asked for some kind of amendment to the existing law. The reason that we have three branches of government is to prevent precisely this kind of abuse.

MARGOT ADLER: Arguments about constitutional law aside, what harm comes from listening to Americans' emails and phone calls. Anti-war organizer Parkin argues that widespread federal government spying and infiltration discourages dissent by law abiding people.

SCOTT PARKIN: I think it's something that impacts people dissenting against their government's policies, whether it's an environmental policy or whether it's the war in Iraq. I think it creates this kind of like atmosphere of fear. So if it could happen to me, then it could happen to lots of other average people out there.

REESE ERLICH: The ACLU lawsuit and a similar one filed by the Center for Constitutional Rights will be heard by federal district judges in Michigan and New York. The Justice Department has until March to respond to the filings. For Justice Talking, I'm Reese Ehrlich.

MARGOT ADLER: Let's take some time now to talk more about the arguments for and against the President's actions. Brad Berenson and Geoff Stone are with me to share their differing perspectives and to help explain the legal arguments and implications of President Bush's domestic surveillance program. Brad Berenson served as Associate Counsel to President George W. Bush from 2001 to 2003. His responsibilities included detainee policy and anti-terrorism legislation. He joins us from Washington, D.C. which is also where he practices law. Welcome to Justice Talking, Brad.

BRAD BERENSON: Thanks so much, Margot.

MARGOT ADLER: Geoff Stone is a law professor at the University of Chicago where he teaches constitutional law. His most recent book is "Perilous Times: Free speech in Wartime from the Sedition Act of 1798 to the War on Terrorism." He joins us from Chicago. Welcome, Geoff.

GEOFF STONE: Delighted to be here, Margot.

MARGOT ADLER: Brad, before we get into the debate over whether the President's domestic surveillance program is legal, let's cover some of the basics of how intelligence is gathered, both here and abroad. First, what does the NSA do?

BRAD BERENSON: Well, as I understand it, the NSA is in the business of gathering signal intelligence, that is intercepting and analyzing communications. And they're doing that in an international context. So, they do not generally have a role with respect to communications that are purely here in the United States or purely for law enforcement purposes. This is part of the Department of Defense. It's an intelligence agency. And its job is to monitor worldwide communications to try to get the intelligence that will be useful to the Department of Defense, to the intelligence community.

MARGOT ADLER: Now, how does the NSA interact with the FBI, with the CIA? How are their duties different? And do all of them report to the President? Do they coordinate their efforts?

BRAD BERENSON: Well, they all ultimately report to the President. And coordination among them is supposed to have been much improved since 9/11. And the sharing of intelligence between the NSA and sister agencies, whether the FBI or the CIA, is also supposed to have increased since 9/11. That's part of that mission of connecting the dots and sharing intelligence that was thought to be so important after the events of 9/11 in which the passage of the Patriot Act was meant to encourage and endorse.

MARGOT ADLER: Geoff, we're going to spend a lot of time on this show talking about a domestic surveillance program that was recently revealed. Can you briefly explain what the program did?

GEOFF STONE: Well, one problem, of course, is that we don't know what the program is in any detailed sense, because that has been kept secret. What we do know is that the

President authorized the National Security Agency to use electronic surveillance to intercept communications involving American citizens on American soil with individuals overseas who were allegedly believed to be in some way connected to terrorism.

MARGOT ADLER: Brad, the President claims that the National Security Agency acted appropriately and that his orders are legally justified. Help us understand the administration's position. Where does President Bush get the authority to operate this program?

BRAD BERENSON: The administration has principally relied on two sources of authority for this program. The first is statutory and the second is constitutional. First, they point to the Congressional authorization for the use of military force in the immediate aftermath of 9/11 empowering the executive branch to use all necessary and appropriate force against Al Qaeda and its confederates for the purpose of stopping, preventing and stopping, any further attacks against the United States. The second source of authority that the administration identifies is Article 2 of the Constitution itself, in particular the Commander in Chief clause which makes the President the Commander in Chief of our armed forces. And according to the administration, thereby gives him certain powers that Congress cannot take away to guide the conduct of armed conflicts like the one that we're engaged in with Al Qaeda.

MARGOT ADLER: Geoff, you and a dozen other legal scholars wrote a letter to Congress expressing your concerns about the spying program. Why do you believe that the administration's program is illegal?

GEOFF STONE: Well, there are primarily two reasons why we believe it is illegal. One is there is a serious question as to whether it is consistent with the Fourth Amendment to the Constitution which prohibits unreasonable searches and seizures which has been construed with respect to electronic surveillance of conversations to mean in the past that that requires a warrant and probable cause. The Supreme Court has never directly decided the question of foreign intelligence operations and whether there maybe any exemption under the Fourth Amendment from the ordinary warrant and probable cause requirements.

But I think the better view in my own sense is that the Fourth Amendment does not provide a blanket exemption for an intelligence investigation. And although there maybe specific circumstances where that's appropriate, that they would have to be very narrowly defined. And in any event, under existing law, certainly existing law from the Supreme Court, there's no basis of such an exemption.

And second, and much more specifically, Congress in 1978 enacted the Foreign Intelligence Surveillance Act which specifically identified the procedures that the government must follow engaging in foreign intelligence investigations, particularly with respect to electronics surveillance.

MARGOT ADLER: We'll come back to FISA a little later. But the ACLU and the Center for Constitutional Rights has filed lawsuits challenging the NSA spying program. And I want

to bring in Maria LaHood who's a staff attorney at the Center for Constitutional Rights. She's a plaintiff in their lawsuit against the Bush Administration. Maria, welcome.

MARIA LAHOOD: Thank you. Thanks for having me on.

MARGOT ADLER: Maria, as a plaintiff in this case, you say that you have reason to believe you were spied on. Why?

MARIA LAHOOD: I represent Maher Arar who's a Canadian citizen who was born in Syria who U.S. officials picked up in September of 2002 while he was transiting through a New York airport on his way home to Canada. They detained and interrogated him for a couple of weeks, interfered with his right to counsel, the Canadian consulate and the courts and then woke him up at 4:00 in the morning, put him in ... had him in shackles, gave him an order saying that based on classified evidence, he was found to be a member of Al Qaeda. And they were not going to end him back to Canada where he lived, but to Syria. In Syria, Maher was interrogated and tortured and held in a cold, dark, underground, grave like cell which was about 3 feet by 6 feet by 7 feet. Finally, after a year, Syria released Maher announcing that he has no links to Al Qaeda. The Canadian government has also said they found no links to Al Qaeda.

MARGOT ADLER: But you believe that you were spied on because you've been making transatlantic calls in regard to this case or what?

MARIA LAHOOD: Right. As his attorney, I communicate frequently with him through email and through telephone. And he lives in Canada. So I would be frankly astounded if our communications weren't being intercepted.

MARGOT ADLER: You can't prove that you know for certain if the government has been listening in on your calls, correct?

MARIA LAHOOD: I don't know for certain, no. I mean, it's the kind of thing where, well, if they're saying he's a member of Al Qaeda, I'm not sure frankly which would be worse. Are they trying to intercept his phone calls? And are they doing it illegally? Our communications are confidential. I represent him. I'm his attorney. I'm ethically bound to keep them confidential. So even though Maher has nothing to hide, I have to think about litigation strategy. And in all of these cases, in CCR's cases, it's not just that the government's listening. But it's that the government officials are actually the defendants in the cases.

MARGOT ADLER: Now, the government suspected that your client was a member of Al Qaeda. Why shouldn't the government be taping any of his telephone conversations, whether it's with you or anyone else?

MARIA LAHOOD: Well, they should be doing it legally. They should be getting a warrant. They should be going to the FISA court if they want to do that.

MARGOT ADLER: And you know that you haven't ... they haven't done that.

MARIA LAHOOD: I actually ... I don't know. I mean, like it has been said, this program is secretive. So it's impossible for us to know what the scope of it is. But we do believe that the likelihood is that the government is monitoring these communications.

MARGOT ADLER: What do you hope to get out of this case?

MARIA LAHOOD: Well, we hope to stop the program. We also hope to find out what communications the government has been listening to with regards to, you know, us, the client.

MARGOT ADLER: Well, thanks, Maria, for talking with us.

MARIA LAHOOD: Thank you.

MARGOT ADLER: Brad, Geoff, do you think these lawsuits have any chance of success? Why don't you go first, Geoff?

GEOFF STONE: Well, it's very difficult because it's a Catch 22. Basically, the rule is that federal courts do not hear cases unless the plaintiff, the person who's bringing the claim, have standing to file the lawsuit. And standing means that they can demonstrate that they've been harmed in some way by the practice that they are seeking to challenge. And where the program is itself secret, it's of course virtually impossible to prove that you have been harmed.

And that has proved to be a real obstacle in the past to individuals who want to challenge the constitutionality of government programs of this sort. Because they haven't been able to demonstrate that they were the targets of the allegedly unlawful conduct. And therefore, courts have said they couldn't challenge the program. And that does create this kind of circle in which the program maybe unlawful. But there's no one with the ability to actually go into court and have a court determine that question.

MARGOT ADLER: Brad.

BRAD BERENSON: Standing is certainly a significant problem for these plaintiffs. Whatever one thinks of the merits of their underlying legal claims, it's far from clear that they're entitled to bring them and to initiate this litigation. But there's another problem too which is what's known as the state secrets doctrine which is a doctrine that prevents the federal courts in civil litigation from hearing a case where accurately determining it would require the disclosure of state secrets that could harm the national security of the country. Where the government invokes this doctrine, the courts are essentially obliged to dismiss the case. So that civil litigation doesn't become a forum for harming the national security. And this would certainly seem to be a case where that doctrine could be implicated.

MARGOT ADLER: Let's get back to FISA. We were talking about that a little while ago. Let's start with just, you know, some basics. It's an acronym that's been heard a lot lately. Geoff, what is FISA?

GEOFF STONE: Well, FISA was enacted in 1978 after a period of time in the 1960s and early '70s when the federal government was engaged in a widespread unlawful surveillance using the FBI, the CIA, the Army intelligence and the National Security Agency to engage in surveillance of primarily political dissidents during the Vietnam War. And one of the developments that occurred after that to try to prevent those difficulties in the future was the enactment of the Foreign Intelligence Surveillance Act. And what it did is to say we recognize that there are special problems involved in foreign intelligence that call for special procedures, particularly in terms of secrecy.

MARGOT ADLER: Geoff Stone is a law professor at the University of Chicago. Brad Berenson, a former White House lawyer, practices law in Washington, D.C.

Just ahead on Justice Talking, more of our debate over President Bush's domestic surveillance program. We'll also talk about past presidents who've tried to expand their authority during wartime. History hasn't always been kind in looking back at the way they use their power as commander in chief. Stay with us.

MARGOT ADLER: This is Justice Talking. I'm Margot Adler. In December of 2005, the New York Times made public what had been secret. Sometime after 9/11, President Bush approved the use of domestic surveillance by the National Security Agency without first obtaining warrants. But who is being spied on and how? Is the President violating federal law and the Constitution?

We'll continue to look at these questions as we return to our debate over the NSA's domestic surveillance program with Brad Berenson and Geoff Stone. Brad Berenson served as a White House lawyer during the first two years of the Bush Administration. Geoff Stone teaches law at the University of Chicago. I'd like to play a clip of President Bush defending the NSA surveillance program.

PRESIDENT BUSH: This authorization is a vital tool in our war against the terrorists. It is critical to saving American lives. The American people expect me to do everything in my power under our laws and constitution to protect them and their civil liberties. And that is exactly what I will continue to do so long as I'm the President of the United States.

MARGOT ADLER: Geoff, throughout history in times of war, presidents have tried to expand their powers. Lincoln suspended the writ of habeas corpus during the Civil War. FDR ordered the internment of the Japanese during World War II. Truman tried to seize the steel mills during the Korean War. Isn't President Bush just doing what a lot of other presidents have done during wartime?

GEOFF STONE: Yes, I think that's exactly right. It is the case historically in virtually every wartime episode we've had that presidents have reached beyond either wisdom or constitutional authority to attempt to gain power for themselves with the undoubted motive of attempting to protect the nation. But one of the difficulties is that the President is in a position where his primary incentive, both for political reasons and for constitutional reasons, is to essentially protect the nation. Rather than in these circumstances to be as sensitive as perhaps he should be to civil liberties.

MARGOT ADLER: So Brad, when we look back on this new expansion of presidential power, will we like the ones that were in history, look at it and say, you know, we're not really proud of this? How will history view this?

BRAD BERENSON: This is not in the same category at all. Indeed, I would argue that this isn't even an expansion, even a slight expansion, of the powers that presidents have historically exercised, not only during wartime, but even during peacetime. In the early 1990s, for example, President Clinton engaged in the warrantless entry of a person's home. That person was Aldridge Ames. He was a spy. And that warrantless entry of his home generated evidence that was used to convict him of spying on the United States.

President Clinton did that quite properly in an exercise of his own inherent national security authorities. And that's a far greater intrusion, here in the United States, physical entry into someone's house, than anything that President Bush is doing now.

MARGOT ADLER: Geoff, has the Supreme Court given us any guidance during these earlier times in history that might be useful in understanding the legal limits of presidential power?

GEOFF STONE: Well, certainly insofar as the question is the President's authority under Article 2 as Commander in Chief, the most useful guidance that the Supreme Court has given came in the Truman field seizure case in a concurring opinion by Justice Jackson. Jackson recognized that the President certainly does have authority as Commander in Chief and that that authority he said should be assessed in part in light of whether the Congress itself has authorized the President's action in which case as Jackson said, the President's power would be at its zenith, whether the Congress has been silent on the question and the President is simply asserting its authority.

And third, whether the President in fact is asserting authority over the express disapproval of Congress. And in that situation, Jackson said the President's power would be at its weakest. Because of the FISA legislation, in my judgment this is exactly the situation we face here that Congress has passed legislation that regulates ... prohibits these types of searches. The President is asserting that he has the authority to do this in defiance of that legislation. And I see no reason in this circumstance why the President should be assumed to have that authority when it has clearly been taken away or never was possessed in the first place, but clearly been spoken to by the Congress.

MARGOT ADLER: Brad, you know, I'd love you to respond to this. And one of the things that I keep on thinking about ... and this is, you know, just as a layperson, is I keep on thinking is the Constitution something that is fine for times where we're safe and feel at peace? And basically, every time we're in a wartime situation, we just can abrogate it?

BRAD BERENSON: No. Nobody, including anyone in the administration is saying that the Constitution doesn't apply in time of war or that there is somehow a wartime exception to the legal restraints that exist in the Constitution. Instead, it's important to understand that the constitutional structure and design address matters of domestic law enforcement and matters of foreign armed conflict very, very differently. And the President's powers in the latter realm are much broader and are indeed extremely broad by design. Because the framers of the Constitution when they sat down to prepare the document had in their personal memories the searing experience of the Revolutionary War where our military efforts had been hobbled in part by the executive was not strong enough when we were fighting off the British.

In the realm of foreign war, the President has got to be able to make operational decisions, whether that's gathering intelligence against the enemy or directing our troops where and how to hit the enemy without seeking the prior approval of Congress or certainly the judiciary which is the least suited of all to be regulating the President's exercise of his powers as Commander in Chief.

MARGOT ADLER: We need to go. But thank you both for a great discussion. Geoff Stone is a law professor at the University of Chicago. Brad Berenson, a former White House lawyer, practices law in Washington, D.C. Thank you.

BRAD BERENSON: Thanks for having me.

GEOFF STONE: Pleasure.

MARGOT ADLER: Tell us what you think. Do you think the President was right to authorized warrantless surveillance? Do you feel safer? You can join the debate on our website, justicetalking.org.

MARGOT ADLER: Spying is a favorite theme in novels and movies. But most Americans don't think too much about whether their phone calls are being monitored or whether the government is reading our emails. Regardless of how much you may or may not worry about being spied on, have you ever wondered how it works? How does the government listen in on and read our communications?

To answer these questions, I called Patrick Radden Keefe. Patrick is a fellow at the World Policy Institute and author of "Chatter, Dispatches from the Secret World of Global Eavesdropping". Patrick, what exactly is wiretapping? How did it work twenty years ago? And how is that different today?

PATRICK RADDEN KEEFE: Well, part of what's funny is that when we hear about the debates that have gone on recently, the word that we always use is wiretapping. In fact, that's kind of a misnomer. It may have started out with government agents actually tapping copper cables, copper wires, that the communications ran through. But these days, a lot of communications interception is much more sophisticated and is a matter of actually snatching signals, electromagnetic signals, right out of the air.

MARGOT ADLER: So is that what they mean when they say data mining? Or is that something else?

PATRICK RADDEN KEEFE: Well, data mining is more complicated. In a way, the paradigm here is the needle in the haystack. So the NSA, U.S. intelligence generally, but the National Security Agency in particular, has been able for years to intercept millions and millions of communications everyday, phone calls, emails, faxes, telexes. And they do this in a variety of different ways, using a lot of different technologies. Data mining is once you've collected that enormous haystack of information and communications, how you sort through it and find the particular phone call, the particular emails, the particular patterns of information that are going to be useful to you.

MARGOT ADLER: Now, when you looked at these telephone calls, either land lines or cell phones, how do they actually get the information?

PATRICK RADDEN KEEFE: The one interesting little tidbit is that if you look around the country at the ground stations that are used to convey satellite communications in and out of the United States, often with 60 or 70 miles of a ground station, there is also a secret NSA base. And if you think about the signals, it's almost like just putting a cup out in the rain. You can collect these signals as they come down from satellites.

But what's interesting about the recent revelations is that we found out that in fact this new program was done with the collusion of some of the major telecommunication carriers in the country. In fact, there wasn't any need to be sneaky about it. There wasn't any need to actually setup bases that could intercept these signals. You could in fact just get the companies to build a backdoor into the communication switches.

MARGOT ADLER: So they called up Sprint, they called up AT&T, they called up Microsoft? I mean, what did they...

PATRICK RADDEN KEEFE: That is the suggestion. I mean, what we know certainly from James Riden's recent book which has come out ... he's the reporter from the New York Times who originally broke the story and has a book which expands on the story ... is that this was done with the cooperation at the level of CEOs of some of the major telecom carriers in the country. So it would be companies like Sprint and Verizon. He has not named the specific company.

MARGOT ADLER: What about emails? How does that work?

PATRICK RADDEN KEEFE: Well, emails are picked up similarly by trying to build taps into the kind of particular junctures that they're routed through. So if you think about the Internet, it's a dispersed network. But a lot of traffic goes through these Internet exchange points. And if you can build a tap into one of those Internet exchange points, that's a place where you can collect millions and millions of emails.

MARGOT ADLER: That brings up a question. For example, suppose I wrote the words jihad and bomb in an email. Would it get flagged?

PATRICK RADDEN KEEFE: It might. I mean, we do know that the technology exists, certainly with emails, to sort through and find words ... not just words, but patterns of words that could be of interest and that that would be one way if you're intercepting millions of emails, to find the ones you're interested in. When I asked a guy who had worked with at NSA, I said, so you intercept all these communications. What kinds of technologies do you have to sort through it? I mean, explain to me how this works. And he said, go to Google. Just go to a regular search engine. And play around with some of the advance search features. And then imagine that you spent ten years perfecting it. That's the kind of stuff we have.

MARGOT ADLER: So give me an example. What does that mean?

PATRICK RADDEN KEEFE: Well, what it means is that you wouldn't ... it wouldn't necessarily be that you would be looking for words like bomb and jihad. I think in large part because the terrorists themselves are quite sophisticated at this point, I mean, they're not so simple as to use words like bomb and jihad in emails precisely because they know we would be listening.

MARGOT ADLER: I was wondering about that.

PATRICK RADDEN KEEFE: Yeah, exactly. The danger there also in fact is I spoke to a number of people in the intelligence community who said that on a number of occasions following 9/11, do you remember in 2002 and 2003, there were instances where suddenly the terror alert level would spike and there would be an indication that something might be happening in Boston this weekend or something might happen in New York on New Year's. On a number of those occasions, people from the intelligence community have told me these were in fact false alarms deliberately put out by the terrorists on lines they knew were being monitored.

MARGOT ADLER: Wow. So what would flag them? I mean, obviously if I said bomb and Jihad, you know, 2,000 times, maybe it would be flagged.

PATRICK RADDEN KEEFE: It might well be. In fact, the system that is used to intercept a lot of communications outside the United States is known as echelon. And in 2,000, there were a bunch of privacy advocates who were very opposed to this system. And they had something called jam echelon day. So what they did was the privacy advocates around the

world organized over email. And they decided that on one given day, they would all write bomb, bomb, bomb, jihad, Osama bin Laden, you know, what have you, in order to try to shut the system down just by virtue of the sheer number of threats they threw out.

MARGOT ADLER: And do we know what happened?

PATRICK RADDEN KEEFE: We don't. And we never will.

MARGOT ADLER: What are some ways that Al Qaeda operatives try to thwart American intelligence gathering?

PATRICK RADDEN KEEFE: Well, this is one of the interesting aspects of this whole story is that in fact Al Qaeda, despite in some respects very backward way of approaching the world, has really embraced modern communications technology. And so, they do everything from use disposable cell phones, so they'll constantly be using new cell phone numbers and will make it much more difficult for U.S. authorities to track them, to all kinds of encryption where they actually encode their communications in ways that will be difficult for us to break.

MARGOT ADLER: I'm wondering, many people who are looking at this domestic spying program and thinking about it are thinking how likely is it that my phone calls overseas are actually being monitored? What would you tell them?

PATRICK RADDEN KEEFE: Well, I think that there is some likelihood. But you need to differentiate between a computer picking up a phone call and an actual human analyst listening to it. So one thing we've learned from this story is that the kind of eavesdropping that was going on was sort of wholesale. I mean, it was really that you build a little tap into a communication switch and you listen to everything that comes through. But the suggestion that actual people at the NSA, actual flesh and blood human beings, would want to sit down and listen to your conversations if you were an innocent person I think is a little bit misguided.

MARGOT ADLER: When you think about the future, what do you think spying technology will be like twenty years, thirty years, down the road? What's being developed right now?

PATRICK RADDEN KEEFE: The silver bullet right now for the intelligence agency is only a desire to develop a crystal ball if you imagine. I mean, you want a system, a kind of all embracing surveillance technology system, that is so effective and so fine tuned that anytime anything happens that somebody on a lapsed Visa applies to take a flight training class or somebody else buys a one way ticket and it's somebody that you're curious about, a computer will raise an alarm. And it will do it in a timely way, in such a way that you can actually go out there and stop it. Having said that, I personally am not persuaded that technology really has all the answers for us. So one example of that is we've become very good at intercepting communication. But these communications are often in foreign languages. And it's really hard for us to figure out what's being said because computers cannot adequately translate all of that for us yet. So a kind of an alarming statistic is that it

emerged several months ago that the FBI has a big backlog of communications which is intercepted between terrorist suspects in the United States. And the communications are in other languages.

MARGOT ADLER: Mostly Arabic I would imagine.

PATRICK RADDEN KEEFE: Well, Arabic, Farsi, Hashka. In a way, Arabic is easy. Once you get into more of your dialect, it becomes even more difficult for U.S. intelligence to rack those. And that backlog of conversations that nobody has translated yet is 8,000 hours long.

MARGOT ADLER: Wow. Patrick, thank you so much for being on our show.

PATRICK RADDEN KEEFE: Thank you.

MARGOT ADLER: Patrick Radden Keefe is a fellow at the World Policy Institute. And he's the author of "Chatter, Dispatches from the Secret World of Global Eavesdropping". To learn more about domestic spying and executive powers, check out our website justicetalking.org.

MARGOT ADLER: Over the last several months, we've made some changes to Justice Talking. And we'd like to know what you think. Are we covering the topics you think are important? Do you have suggestions for issues you'd like us to discuss? Let us know what you like and don't like about what you hear. Email us at comments at justicetalking.org. Thanks for joining us. I hope you'll tune in next week. I'm Margot Adler.
