November 20, 2013

Andrea Bussell | 718.522.7171
abussell@shorefire.com
Rebecca Shapiro | 718.522.7171
rshapiro@shorefire.com
Mark Satlof | 718.522.717
msatlof@shorefire.com

Intelligence Squared U.S.

Spy on me, I'd rather be safe

For the Motion: Stewart Baker, Richard Falkenrath
Against the Motion: David Cole, Michael German
Moderator: John Donvan

AUDIENCE RESULTS	
Before the debate:	**After the debate:**
26% FOR	**29% FOR**
41% AGAINST	**62% AGAINST**
33% UNDECIDED	**9% UNDECIDED**

Start Time: (17:36:03)

John Donvan:
And -- and as I said, we are delighted to be doing this debate in partnership with the McCain Institute for International Leadership. And I would like to welcome to this lectern the Institute's executive director, Ambassador Kurt Volker.

[applause]

Kurt Volker:
Thank you, John. Thank you very much. Delighted to be here and delighted to be partnering with Intelligence Squared again. We've done another debate together on defense budgets. The McCain Institute for International Leadership is a part of Arizona State University, based in Washington, D.C. with a strong footprint in Arizona as well. And in fact, during the course of tonight's debate, we have students who will be watching this at ASU. And it will be broadcast on Arizona State television as well. We seek, at the McCain Institute, to advance the next generation of character-driven leadership. That is our core mission. And part of that core mission is to advance the culture and the practice of serious debate over serious issues affecting our country.

We've launched this debate series at the McCain Institute back in January with debates on Syria policy and Afghanistan.

17:37:04

We're delighted to be doing this one with Intelligence Squared. We have another one on December 5th. Please come, this room, December 5th, on drone policy: Are we going too far? I'm confused now about the hash tags because if you want to Tweet, and you can do it without interfering with the signals, then it's hash tag spy debate. But if it interferes, don't do that. John, what was the signal you showed for spontaneous applause?

[applause]

Thank you.

John Donvan:
Yeah, what we're really counting on is limited Tweeting competence in the audience. So --

[laughter]

So if you can, we're delighted, but if you're not, we just want you to shut down. And just to get us started, I just want to, one more time, give a round of applause to Ambassador Volker for bringing us here.

[applause]

17:38:01

A metaphor: The U.S. government sucking in all of that data about the phone calls that we make when we're talking, who we're talking to, how long we're talking, is a fishing trawler dragging a net across the high seas. The government and its crew at the National Security Agency wants to catch bad guys, terrorists the crew on the fishing boat wants to catch, let's make it tune a fish. But the fishermen's net also drags along with it all those good guys who are swimming out there, those cute little dolphins. And the dolphins die, which is a clear harm to them. But is there a harm to us in the data that is collected by the NSA in its net. Nobody likes it, but nobody dies from it. In fact, the argument is that the NSA's big net is saving lives, keeping all of us little dolphins out there safe. Yes? No?

Well, it sounds like there's a debate in that, so let's have. Yes or no to this statement: Spy on me, I would rather be safe. A debate from Intelligence Squared U.S., in partnership with the McCain Institute for International Leadership.

17:39:07

I'm John Donvan. We have four superbly qualified debaters, Americans all. But two against two in this debate for and against this motion: Spy on me, I would rather be safe. We look at this motion not as an extreme statement, all for spying and all against spying. But we're going to be talking about gradations, what's in the middle. As always, our debate goes in three rounds, and then the audience votes to choose the winner and only one side wins. Our motion is, "Spy on me, I'd rather be safe." Let's meet the team arguing for this motion. First of all, ladies and gentlemen, please welcome Stewart Baker.

[applause]

And Stewart, you were the NSA's top lawyer, and later on, you became the first assistant secretary for policy at the Department of Homeland Security. And in your memoir, "Skating on Stilts," you wrote about having to build the whole thing from scratch, recruiting the right people, setting up a budget.

17:40:03

And at the end of it, you wrote this: "I did that. Now I'm tired."

[laughter]

So have you caught up on your sleep?

Stewart Baker:
Well, I may never be tan, but I'm rested, and I'm ready.

John Donvan:
All right. Ladies and gentlemen, Stewart Baker.

[applause]

John Donvan:
And, Stewart, your partner is?

Stewart Baker:
Oh, Rich Falkenrath -- with whom I worked at the Department of Homeland Security, and one of the people I admired most in my government service.

John Donvan:
Ladies and gentlemen, Richard Falkenrath.

[applause]

Richard, you are also arguing for this motion: Spy on me, I'd rather be safe. You've held a lot of leadership positions in U.S. counterterrorism efforts. You were deputy Homeland Security advisor under the Bush administration. You were New York City's police department's deputy commissioner for counterterrorism. Both jobs, tough places, tough times. But which is the harder place to live in, New York or Washington?

17:41:05

Richard Falkenrath:
Washington's harder. I'll take traffic gridlock over partisan gridlock any day.

John Donvan:
Ooh, clever, clever. Ladies and gentlemen, Richard Falkenrath.

[applause]

John Donvan:
Our motion is this: Spy on me, I'd rather be safe. We have two debaters now arguing against this motion. First, let's welcome, please, David Cole.

[applause]

John Donvan:
David, you are a professor of law at north town university law center. You are one of the country's leading civil liberties advocates. You've litigated many Constitutional cases, big ones, in front of the Supreme Court. We read that when you off to law school, you did not actually plan on being a lawyer, but you were going to be a writer. So you didn't, so I'm wondering, is the nation missing one great American novel?

David Cole:
Well, I think it turns out the truth is stranger than fiction. If I'd written a novel saying the NSA was spying on every one of us, no one would have believed it.

John Donvan:
Thank you.

17:42:02

[laughter]

John Donvan:
Thank you, David Cole.

[applause]

John Donvan:
These guys are on fire already. And your partner is?

David Cole:
Mike German, one of the few people in the world who's worked for both the FBI and the ACLU.

John Donvan:
Exactly.

[laughter]

Ladies and gentlemen, Michael German.

[applause]
Yeah. You worked for the FBI for 16 years. You were a special agent in domestic terrorism for 12 of those years. Then you moved on, and you resigned in 2004. And now you work for policy -- on policy for the UCLA -- the UCLA.

[laughter]

Now you're working for -- on policy for the ACLU. And I'm just wondering, does -- how does being -- having all that undercover experience come into play for you now?

Michael German:
Well, the first rule of working undercover is never telling anyone you've ever worked undercover.

John Donvan:
Oh. Boy, did I make a mistake. Well, ladies and gentlemen, Michael German.

[applause]

So those our -- those are our debaters. And our motion is "spy on me, I would rather be safe." And this is say debate. It's a contest.

17:43:03

These two teams are competing for your votes. And by the time this debate has ended, we will have asked you to vote twice, how you stand on this motion. And at the end of the debate, the team whose numbers have been changed the most in percentage point terms will be declared our winner. So let's go to the preliminary vote. Go to the key pads at your seat. And you look at the motion and the team arguing for it, this side -- the motion is "spy on me, I'd rather be safe. If you agree with that motion, push number one. If you're on the other side at this point, if you're against this motion, push number two. And if you're undecided, a perfectly reasonable position, push number three. You can ignore the other keys. They're not live. And if you push the wrong button, just correct yourself, and the system will lock in your correct vote -- your last vote. And then at the end of the debate, we're going to go through the process again, and we get a readout in about 45 seconds to a minute and a half.

17:44:04

So you'll know -- we'll know who the winner is based on whose numbers have changed the most in percentage point terms. So we go in three rounds. And now we go onto round one, opening statements from each of our debaters in turn. They will be six minutes each. Speaking first for this motion, "Spy on me, I'd rather be safe," Richard Falkenrath. He is a principal at the Chertoff Group and former New York City Police Department deputy commissioner for counterterrorism. Ladies and gentlemen, Richard Falkenrath.

[applause]

Richard Falkenrath:
Thank you very much, John. Thank you all for coming. These issues we're debating tonight are difficult and very complex. They engage some of the most fundamental issues in American public life: Liberty, security, technology, democracy. And there really are no simple answers to this. We'll do our best to distill it, but let me just say, anyone who's worked in these issues in a practical way knows how hard they are and that they do need to be very carefully weighed and not handled impulsively or ideologically.
17:45:11

I'm going to make three points in this opening statement. The programs that we're going to talk about tonight really do matter for security. And for me, having been deputy commissioner of counterterrorism at the NYPD and then three different jobs in the White House before, during and after 9/11, I can really tell you this on a first hand basis.

And we may get into some of the details of how this works, how these sorts of systems lead to the original lead that then leads to the unraveling of a plot and the saving of lives. It is not abstract. It is real no kidding lives at stake sort of business. I don't want to hyperventilate about it, but I've lived through enough of them to be able to recount some of the direct experiences. And if that comes up in a Q&A, we'll have to go through them in greater detail. But they really do matter. Turns out a terrorist plot is not that difficult to stop if you know about it, and finding out about it in the first place is by far the hardest step in the process.

17:46:10

In the overwhelming number of incidents that we've had since 9/11, that original lead, what's called the "predication for further investigative steps," has come from electronic surveillance of one form or another, so these programs really do matter. Second, and what I'm about to say I think is going to unite both sides of this debate. Stewart and I have worked on these issues for a while. We are for lawful surveillance, lawful forms of electronic surveillance, things which clearly backed up by the Constitution, by statute, and by court interpretation are permissible, so don't for a second think that Stewart and I are arguing for anything that is illegal. And since the other side I think is very likely not to argue in favor of illegal surveillance either, I think this is something that brings us together. We are for lawful forms of surveillance.

17:47:04

And there is an extensive body of law that governs when, how, where these systems can be deployed. And this is not a legal seminar, but I can tell you that, that system has evolved in such a way, over the last 35 years, that it is really nothing short of an enormous success for the American privacy and civil liberties community. It's hard to believe, but it's a fact that 35 years ago there was no statutory constraint and no jurisprudential constraint on the ability of the president of the United States to conduct electronic surveillance inside the United States for foreign intelligence purposes. It was unfettered. Now it's fettered quite significantly, first with the creation of a FISA court, the Foreign Intelligence Surveillance Court, with -- and an act of 1978, and then adjusted in important ways with the FISA Modernization Acts of the last five years.

17:48:00

And so this is something you really have to understand, if you take this in kind of broader historical context, an incredible amount of progress has been made, and these sorts of programs have been brought under the constraint of law where they were not previously. Previously -- if these laws had never been passed, it was solely the powers of the president under the Constitution, Article 2 that permitted him to do this. And those days are over. Now there is a law which governs it, and many laws, in fact, and the court is involved in overseeing things which previously were exclusively within the

domain of the president. There are now checks and balances on his power to do that, and that is extraordinary progress. And the third thing I want to say is how unusual this area is in Washington. As I said, there's partisan gridlock in here. Name me another issue in public life, health care or taxation or entitlement reform or what to do in the Middle East, where you have the executive branch, the legislative branch, and the judiciary all unanimous about the contours and direction of a specific program.

17:49:06

It's remarkable that this happened, not just the three branches of government but in the case of the executive branch a set of policies and programs which have survived partisan transition. So these programs which we have today emerged in the latter half of the Bush administration and have survived essentially unchanged into the Obama administration, two leaders who could not be more different. And they are unchanged. And so this is where the other side of this debate really have a pretty tough argument because you have broad bipartisan majorities in both chambers of Congress, the two presidents of different parties, different characters, one, the current one, quite liberal and quite educated in Constitutional law -- he taught it, University of Chicago -- and the judiciary all backing up and saying it's fine. So what the other side has to do, and it's a tough burden I think, is say, "They've all got it wrong, we've got it right, we know better." And I think frankly that's a pretty high burden for them. Thank you very much.

17:50:05

John Donvan:
Thank you, Richard Falkenrath.

[applause]

I just want to mention to our other debaters, we give them a visual clock so they know how much time they have left. And our clock's not functioning. Richard, you hit it. You have a magic clock in your head. But if the other debaters would like me to give them a 30-second warning to give you a target, I'm happy to do that. And if you don't think, you know, so I'll just -- I'll just gently say 30 seconds. Okay. I'll do that. Our motion is this: Spy on Me, I Would Rather Be Safe, and our next debater will be speaking against the motion. He is Michael German, senior policy counselor for the American Civil Liberty Union, Washington Legislative Office, and a former FBI special agent. Ladies and gentlemen, Michael German.

[applause]

Michael German:

Thank you. Thank you, John, and just to be clear, the question isn't whether there are threats; there have always been threats and I would be the last person in the world to tell you that there aren't threats right here in our own community that can harm us.

17:51:05

And it's not whether the government should have tools to address those threats -- of course it should. It's whether the tools the government is using today are necessary, legal, or effective. I oppose the motion Spy on Me, I'd Rather be Safe because I'm not a terrorist or a violent criminal, and spying on me isn't going to keep anybody safe. And unless you're a terrorist or a criminal you should also vote no, whether you care about your privacy or not because spying on you is only going to waste security resources and fill important intelligence databases with irrelevant information. Spying on you and spying on me makes us less free and less safe. We know that spying on us didn't protect us from the Christmas Day underwear bomber, from the Times Square bomber, from Najibullah Zazi's crew who got an explosive into New York City, but ultimately flushed it down the toilet rather than detonating it.

17:52:03

These terrorists all traveled to foreign terrorist training camps. Then they came to the United States and attempted to bomb us. Luck is what protected us in these cases, not mass surveillance.

Spying also didn't protect us from the Boston Marathon bombers or shootings at Fort Hood or at an army recruiting center in Arkansas. These terrorists were investigated by the FBI before they went on their rampages and yet they weren't stopped. While the government was spying on us, violence from far right extremists killed 300 people in the United States since 2001. And this is just a tiny fraction of the 14,000 murders that happen in the United States every year. A third of those -- more than a third of those -- go unsolved. Solving 4,000 murders a year? That would keep us safer. In a 16-year FBI career, I can honestly say I never found a criminal or a terrorist by rummaging through the personal information of innocent people.

17:53:04

Traditional law enforcement standards of reasonable suspicion and probable cause don't just exist to protect our rights. These standards actually helped me as an investigator, because they forced me to focus on the right people for the right reasons, to follow evidence rather than flawed hunches or profiles. In my undercover work against neo-Nazis and anti-government militias, there were a lot of people saying things I didn't like, but I knew I had to have a reasonable basis to assume somebody was engaging in violent activity or illegal activity. Otherwise, if I couldn't find that I could just turn my attention to somebody else, because again there are real threats, and this

standard helped me focus my investigations properly so those cases successfully prevented terrorist attacks, ended in successful prosecution, and didn't violate anyone's rights. Today our government's spying on all of us in a lot of different ways.

17:54:05

It collects all of our telephone records on an ongoing daily basis. It photocopies every piece of domestic mail, it intercepts Americans' international communications and financial transactions, it collects millions of images from license plates readers and surveillance cameras. The FBI even collects census information so it can map American communities by race and ethnicity. The problem with these programs -- the problem is that these programs collect so much information that the signal gets lost in the noise. So it's not a surprise that the NSA can point to only one terrorism-related prosecution that might not have happened absent gobbling up all of our telephone numbers, and that was a material support for terrorism case that involved an $8,000 transmittal to Somalia. Think of the billions of dollars these programs cost and how that could have been spent on so many different things, including things that improve security.

17:55:06

If a 2011 triple homicide in Waltham, Massachusetts had been solved the Boston Marathon bombing might never have happened. Instead of making us safe, these mass surveillance programs cast undeserved suspicion on innocent people, simply because they're linked somehow to a suspect -- not a terrorist, but suspect, often by two or three degrees of separation, like that old Kevin Bacon game. This process creates a flood of false positives that then have to be run to ground. These are what the FBI used to call the "Pizza Hut leads" because they often ended up at the pizza delivery guy. The difficulty resolving this false suspicion leads to bloated watch lists, the watch list, over a million names on it now, but often not the right names, like the Underwear Bombers. The flood of data coming into the intelligence community is so overwhelming the agents that it's harming our security.

17:56:04

The National Counterterrorism Center says it receives 5,000 pieces of information and puts 350 people on the watch list every day. The official review of the FBI's investigation of Major Nadal Hassan prior to the Fort Hood shooting blamed what is called "the relentless workload on the agent," which was caused by --

John Donvan:
30 seconds.

Michael German:

-- what it said was a data explosion within the FBI. The FBI assessment of Boston Marathon bomber Tamerlan Tsarnaev was one of 1,000 assessments the Boston JTTF did that year. A study of intelligence community analysts published earlier this year included some interesting quotes. One analyst said, "There's just so much information. How do I know which of 3,000 cables to pay attention to? It's an unrealistic expectation."

17:57:00

John Donvan:
Michael German, I'm sorry, your time is up. Thank you very much. Michael German.

[applause]

And here's where we are. We are halfway through the opening round of this Intelligence Squared U.S. debate. I'm John Donvan. We have four debaters, two against two arguing it out over this motion: Spy on me, I'd rather be safe. You have heard from the first two debaters, and now onto the third. And Stewart, our clocks are working again. Is that going to be enough for you?

Stewart Baker:
That'll be fine.

John Donvan:
You don't want the audible. Okay. Thanks. Here's -- I'm going to introduce you. Here to debate for the motion, "Spy on me, I'd rather be safe," Stewart Baker. He is former general counsel of the NSA and the first assistant secretary for policy for the Department of Homeland Security, currently a professor -- currently a partner at the law firm, Steptoe and Johnston. Ladies and gentlemen, Stewart Baker.

[applause]

Stewart Baker:
Thanks, John. Mike German has put the problem, I think, as directly as it could be. When, if ever, is it appropriate for the government to gather data on large populations, everybody in order to make us more safe?

17:58:08

So that's the question. You can call it spying on everybody, if you like, and he does. But it's not as unusual or as ineffective, and certainly not illegal as he suggests. And I'll take his challenge of saying, "When has spying on everybody -- when has gathering all of the data on everybody, innocent or not, helped us stop terrorist attacks?" and let's take the Zazi case, the Times Square bombing case, the Underwear Bomber.

When I was at DHS, one of the things we fought very hard to do was something that I think Mike German would call spying on everyone. We said we want the airlines to give us the travel reservation information and the passport information on everybody who's flying into the United States; everybody, not just the suspects.

17:59:07

We need to know who's coming here. We use that data to compare the names and the information that was on there to the databases in which we had information about people we were worried about, or patterns that we were worried about. And then when those people arrived, a few of them, half of a percent, would end up spending about 45 minutes talking to a customs agent about why they were coming to the United States, who would try to determine whether this person was a threat. That was a routine practice. And most of us just, you know, it's welcome home, and you move on. But a few people, they couldn't stop everybody, but they could stop a few people. They used this data to decide who was worth worrying about. Now, let's take the Underwear Bomber.

18:00:02

The people who did airport security had no information about him. And not surprisingly, didn't check in very carefully, and he got right past them. It turned out that when he was due to land, he had already been flagged by the customs folks who had access to that data as somebody that they, through checking back in databases, were able to identify as somebody that they were worried about. So he would have been caught if we'd had the information earlier, and he would have been caught when he landed. That's, indeed, probably why al-Qaeda wanted to blow up the plane before he had to get past the customs officials.

The same thing is true for the Times Square Bomber, where after the bombing, the FBI got a phone number. They asked our guys, do you have that phone number? Did anybody with that phone number come into the United States? Turned out that he'd given that same phone number to the airline for his reservation data.

18:01:02

The department was able to identify him, provide the data, start a man hunt. And then he got on the plane and was about to leave the country. The only reason we caught him is because we had data on everybody who was getting on that plane, and we were able to run the information in the background and determine, this is the guy we're looking for. He's on the plane. That plane had already closed its doors when the customs officials went on to pull him off. He would have gotten away, but for the data which Mike German calls, "Spying on everybody." I would call it "gathering data that is already

in the hands of third parties," given it to the airlines, they're going to use it to decide whether you get chicken or tornadoes, and whether you get that 3 inches of extra leg room. You know, I'm happy to have that information also used to make sure I actually arrive at my destination.

18:02:01

And it seems to me that the intrusion -- you can call a lot of scary things, but the fact is, at the end of the day, it's information that I willingly shared with the airlines, and I'm happy that they're using it to protect me as well. That's the real question we have here, is, can we use data that we've given to a third party, can the government use data that you've given to a third party, to try to find terrorists? We do that all the time. The NSA program is probably the most aggressive use of that. But at the end of the day, this is billing information you've given -- we've all given to the phone companies. It is searched by law enforcement outside of the NSA program 1.3 million times a year. What the NSA did, at the end of the day, through the program and through the safeguards that they established for that program, they required --

18:03:02

Yes, we gather the information, but no one can search it without articulable, reasonable suspicion passed on by a lawyer. It'll be audited. A limited number of people will have access to it. At the end of the day, 300 numbers went into that on a given year. 500 -- there were searches to find who they were talking to. 500 numbers came out as potentially suspicious. And only then did the government go out to try to find out whose name was associated with those phone numbers. 500 people versus -- and all used for terrorist purposes, all carefully scrubbed versus 1.3 million searches done by law enforcement every day without bringing 1984 home to America. Thank you.

John Donvan:
Thank you, Stewart Baker.

[applause]

Our motion is, "Spy on me, I would rather be safe." And now our final debater making an open statement is David Cole. He will be arguing against this motion.

18:04:03

He's a professor at Georgetown University Law Center, and a volunteer attorney for the Center for Constitutional Rights. Ladies and gentlemen, David Cole.

[applause]

David Cole:
Thank you. Stewart Baker gave a great defense of the public passenger data program that we've all known about for years, and no one has had any problem with. Of course, that's not what's at issue here. What's at issue here is whether we have a problem with the secret NSA program adopted in secret through secret interpretations of a law whose author said this would never -- he never would have dreamed of authorizing this sort of program, had he known that's what the government was going to do with it. I think that's a very different question. The NSA is collecting information on every time every one of us calls or texts anybody; your son, your daughter, your mother, your doctor, your psychiatrist, your AA mentor, your old girlfriend, your new girlfriend.

18:05:11

[laughter]

That's what they're collecting. It's not passenger data about people getting on airplanes. It's literally every phone call. It's doing it in secret, as I said, pursuant to a secret interpretation of a law whose author said this is not consistent with what I understood. And Rich Falkenrath says there's unanimity about this program, I don't think so. There are 30 bills that have been introduced in Congress to try to fix the problem that has now been disclosed not because of openness and checks and balances but because of Edward Snowden leaking it. And this is a program that the NSA lied to Congress to keep secret from us. When the director of National Intelligence, James Clapper , was asked pointblank, "Are you collecting data on millions of Americans?" he said -- in Congress, under oath, he said, "No." Later he said that was the least untruthful answer he could give.

18:06:07

Well, I think I can think of two more truthful answers. One would have been, "Yes," and the other would have been, "We can't confirm or deny." But instead he lied to us, lied to us, why, because if we knew that this program was underway, we wouldn't accept it. Mike has suggested reasons why you should vote against this kind of spying, because it doesn't work, doesn't make us safe. I'm going to suggest that you should vote against the program because it violates core principles of a democracy, transparency, and privacy.

A healthy democracy demands transparency from the government and privacy for the citizens, but it seems that today we have reversed that, with the government demanding transparency from us but insisting on secrecy with respect to the programs that it employs.

18:07:05

We should be concerned about this because of the problems that secrecy poses to a democracy. Of course there's a role for secrecy in terms of national security, but there's also a role for democracy. And when you have an agency engaging in conduct that the person who passed the law says is totally inconsistent with the law he passed and doing it in secret and lying about it, you have a problem with democracy. National security is a compelling state interest, and it is justifiable to engage in surveillance of a range of kinds in order to keep us safe. But we have a right to have a say in how far the government goes in spying on us and our daughters and our sons and our mothers, et cetera. And we were denied that, say, and denied it in the worst possible way, through secrecy and lies.

18:08:06

We should also be concerned about the program because it invades our privacy. Privacy is critical. It's essential to human development. It's essential to intimate relations. It's essential to political freedom. People can't speak freely when they fear that the government may well be listening in. Now, some people say, "Well, you know, if you've got nothing to hide, you've got nothing to fear." But I think most of us have nothing to hide but most of us nonetheless close the door to our bedrooms, close the door to our house, put password protections on our computers. Some of us limit who can be friends with us on Facebook.

[laughter]

We seal the envelopes that we mail. We believe in maintaining privacy because it's central to human existence.

18:09:05

And it's particularly essential to a robust democracy that people have the privacy to engage in political discussion without fear that the government's going to be coming in and invading that privacy. Stewart suggests, "Well, some -- if Verizon has it, why should we be concerned if the government gets it?" Well, I think there are a number of reasons we should be concerned. First of all, Verizon doesn't collect this data on every person and hold it for five years as the NSA is doing. That's precisely why the NSA is demanding it, because Verizon just gets it, looks at it for billing records, and then gets rid of it. Second, Verizon doesn't have the power to lock you up, it doesn't have the power to indict you, it doesn't have the power to investigate you for tax evasion because it doesn't like your politics, which we've seen this government do in the past.

18:10:03

The government does have that power. And, third, Verizon doesn't have the incentive to go after its customers in the same way that government unfortunately all too often has an incentive to go after those that are critical of it. And we've seen it -- we saw it in the '60s and '70s with a national security program that ended up focusing on anti-war protesters, Civil War -- I mean civil rights activists, Martin Luther King, and women's rights activists. So it's not an abstract concern. It's a real concern. So I think because the NSA program turns democracy on its head, demanding that our lives be transparent and insisting on secrecy for the government, you should vote against the motion.

John Donvan:
Thank you, David Cole.

[applause]

John Donvan:
And that concludes round one of this Intelligence Squared U.S. debate where out motion is: Spy on Me, I Would Rather be Safe.

18:11:05

Now you've heard the opening round. Remember how you voted just before the opening round, because we're going to have you vote immediately after all of the arguments and after round three, and the team whose numbers have changed the most over the course of your two votes in percentage point terms will be declared our winner. Now on to round two. Round two is where the debaters address one and another directly and answer questions from me and from you, our live audience here in Washington, DC. We have two teams of two arguing out on this motion: Spy on My, I'd Rather be Safe.

The team that's arguing for this motion, Richard Falkenrath and Stewart Baker, make the argument that there are no simple answers to this; yes, there is a conflict between privacy and security, but that on the whole the mass surveillance programs such as were exposed in 2013 regarding the NSA and phone records and Verizon -- that by and large that those programs work, that they are protected by safeguards. Those safeguards are legally sanctioned and the result of years and years of concern about how to incorporate privacy into the activities -- respect for privacy into the activities of the intelligence community.

18:12:13

The team arguing against the motion, Michael German and David Cole, they're arguing against this motion, Spy on Me, I'd Rather be Safe. They're saying yes, there are threats and there does need to be surveillance, but that basically a government that's able to fish in this sea of data is a government that's exceeding its position in democratic

society. The violation of privacy goes too far. The failure to be transparent goes too far, and that in any case, the system would be flooded with so much data in such a situation that it actually becomes counterproductive to have that information on citizens who have done nothing wrong.

I want to go to the side that's arguing for this motion, that's more comfortable with the surveillance programs that are in place, and say to you that your opponents have made the argument that -- well, one of them in particular, he said this program that the NSA conducted really affronted his sense of privacy, just in a very basic way.

18:13:09

Now you -- your side, you're not denying the fact that to some degree there is a compromise of privacy. It's just not enough to count, and I want to know why that is. Where is your line, Stewart Baker, on just how willing to be spied on you are?

Stewart Baker:
There's no doubt that when the government collects data, everybody in the democracy ought to be concerned and want to make sure that it is handled in as privacy-protected a fashion as possible, consistent with actually having it be effective. The difficulty here is -- or the protections here are built in to the back end of the system. That is to say the government has the data, but just because it has it doesn't mean it's allowed to look at it. It's set up a whole set of rules, court enforced, aggressively audited, limited number of people who can get access to this data, and clear rules for when they can do it.

18:14:08

To make it much more like the rules that apply to ordinary searches by law enforcement, which is you have a suspicion, and you ask a question about the person or the -- in this case, the phone number that you have a suspicion about. They don't have any ability to look at people for --

John Donvan:
So in answer to my question, if the safeguards were not in place, you would have a great deal more concern?

Stewart Baker:
Yes, absolutely.

John Donvan:
All right, so let me take that to the other side. They're arguing that in fact while the data is there, that there are built in safeguards, and those things are for real. You know, there's a process through which governments need to go in -- or that the government needs to know to go in order to dig more deeply into that pile of data, but Michael

German, do you trust in the safeguards? Or what is your response to their basic argument that maybe it's not so nice, but it's safe?

Michael German:
Well, I guess the easy two-word response would be Edward Snowden, right?

18:15:02

If this data and all this stuff was so protected and so well regulated and so controlled, how would Edward Snowden have gotten so much access to it? And luckily, because Edward Snowden did get so much access to it, and because we're still benefiting even this week from information that's coming forward, what has become clearer and clearer is that the FISA court was being -- that the NSA was misrepresenting the program, I'll say that in the nicest way. And continually going beyond the scope of the minimization procedures and rules to the extent that in 2011, Judge Bates said it was unconstitutional [unintelligible].

John Donvan:
Bottom line, then, are you saying that you don't trust the system?

Michael German:
I don't trust any system that doesn't have effective public oversight.

John Donvan:
Richard Falkenrath.

Richard Falkenrath:
It's worth --

[applause]

Richard Falkenrath:
There's a few things that \-- neither do Stewart or I. We think it's effective in this case. And you've left out a few facts. So this program, the one that draws your ire so strongly, the bulk acquisition of telephone call records.

18:16:03

First point: The Supreme Court has held, since the late '70s, that this data, like what number called what number at what time for how long is not privacy information. Getting it from the government is not a search. Now, professor Cole and his scholarship on this is against that and thinks the Supreme Court got it wrong. Nonetheless, the Supreme Court, for 35 years, has held this consistently. Second, going beyond what is strictly necessary from what the Supreme Court says, the Congress has authorized this

provision. It's called section 215. It was in the Patriot Act. It amended the FISA court regulation. People on your side of this debate were against it then, and you're still against it now. 215 was very controversial then. It's still controversial now among the same people. But finally, you leave out the fact that this program, the bulk acquisition of telephone call records for narrow counterterrorism purposes has been authorized 34 times by 14 different federal judges, who wrote, in writing, they said they would not have authorized it but for the safeguards in place. And every 90 days, they have to do it again.

18:17:06

John Donvan:
All right. Let's let David Cole respond.

David Cole:
Well --

John Donvan:
Your opponents are saying it's credible.

David Cole:
What's that -- the first --

John Donvan:
Your opponents are saying the safeguards are very credible.

David Cole:
The first thing I'd say is I'm not sure we would be satisfied even if the safeguards were fully credible and followed in every instance. Suppose the government said, "We're going to put a video camera in each one of your bedrooms. We're going to collect the data from what happens in your bedroom, but we're not going to look at it until we have a really good reason to look at it. Would we say, "Okay, that's fine. Go ahead. Put the video camera in every one of our --" so back end safeguards don't answer all of the concerns. To Richard's point about the notion that this information is not protected -- we don't have a reasonable expectation of privacy with respect to this information. Mike Hayden has said, if they can get all the --

John Donvan:
Just remind people of who Mike Hayden is.

David Cole:
Mike Hayden, the former head of NSA, CIA, has said, “if I can get all of that phone data about who you've called over a period of time, I don't need to listen to what you're saying.

18:18:12

I can get such a portrait of who you are that I don't even need the content. This stuff is more private than the content itself."

John Donvan:
David, but I don't think that I -- I directly heard an answer or an articulated answer to why you don't trust the safeguards that -- you said they're not credible after Richard actually made a pretty good point that the Supreme Court has time and again and legislation -- why don't you find them credible?

David Cole:
Well, first of all, Richard's point about the Supreme Court was -- Supreme Court has not found that the safeguards are credible here. What the Supreme Court found was that in the '70s, before Al Gore invented the internet --

[laughter]

-- it found that when you make these phone calls, you don't have an expectation of privacy with respect to the data regarding who you called and how long you called for. Immediately Congress responded and said, yes, we do have an expectation of privacy.

18:19:02

And they passed a law that forbade the government from getting it without individualized suspicion. This law, the government has now turned around and perverted, in secret, to get the very information that Congress originally said we shouldn't get, and to get not just the data with respect to one suspect, which is what was at issue in the Supreme Court case in the '70s, but to get every piece of phone data of every one of us every time we make a call.

John Donvan:
Richard Falkenrath.

Richard Falkenrath:
Let me try to put this in terms everyone can understand the utility of this. So professor Cole, Mike German, Stewart Baker, John, we're here at the same place, same time, participating in a complex operation. I, in fact, never had a phone call with David Cole or -- nonetheless we're here, doing something relatively complicated. Now, it turns out --

John Donvan:
You mean putting on this show.

Richard Falkenrath:
Yes. We talked to another person.

John Donvan:
You have no idea how complicated it is.

Richard Falkenrath:
We talked to another person, who is in the audience, and was the coordinator of this. And now, here's -- do you understand why this data matters and why Mike Hayden would say that we want this information where you have no expectation of right to privacy.

18:20:05

We talked to the coordinator of this debate, who then put us together, right? That is how plots are unraveled. They find out about one perp. They look at the communications pattern, they identify the network, and they can diffuse the plot. So imagine this was not a debate but a bombing. This is how -- this call record data is how it gets unraveled and stopped. And it's why it matters. And it's not a video camera in the bedroom. That is -- that is not a fair comparison, and I think you know it. This data, for very good reasons, the government and the Congress and the court do not hold that you have the same expectations of the right to privacy as to you do in your bedroom.

John Donvan:
Let me bring in Michael German and move the topic a little bit to the issue of practicality, because Michael, you made the case in your opening statement against this motion, "Spy on me, I'd rather be safe." You made the case that the flood of data is actually -- it's overload, that it can't be used. And yet we heard Stewart Baker, your opponent, get up and go through a number of cases that he worked where in fact he has --

18:21:02

He clearly argued that the availability of the data after crimes were committed helped track down -- put together how the plot was put together and make some pretty decent arrests.

Michael German:
So there's no doubt the FBI has tremendous investigative skills that can be put to place once you know something bad has happened. And I've seen that done on a personal basis. But what we're talking about -- first of all, it was sold as a preventive measure. This is for preventing terrorism, to the for solving a terrorist bombing. So you know, I think that the analysts at the NCTC really say it all. So another I was going to quote.

"There are so many databases, people don't even know what buttons to push. They don't know where to get information, or they may even already have it and not know it." Another said, "More information isn't necessarily better. Better information is better." So that's what we have to focus on, how -- how do we let law enforcement have the tools it needs to get the bad guys without impacting the rights of the rest of us?

18:22:02

And I think the founders did a pretty good job of setting up a system based on reasonable suspicion and probable cause.

John Donvan:
But does that mean you're just dismissing the achievements that your opponent laid out, where in fact the data was used to --

Michael German:
Again, there's no transparency. There have been these cases that they say these were solved with this program --

John Donvan:
So you you're telling me we don't know whether he's telling the truth.

Michael German:
Right. Because --

John Donvan:
Not that you're -- and I want to make clear --

Michael German:
No, no.

John Donvan:
-- that you're not calling -- accusing him of dishonesty. What I'm saying is there's no check to know whether the story is true or not.

David Cole:
and it's also worth noting that Stewart did not say that the NSA data mining program solved any of these. What he said was the passenger data program. When the NSA was asked, point blank, by Congress, and by a friendly member of Congress, can you tell us some terrorist plots that you've stopped by virtue of the NSA data mining program? The call data program, he said, "Yes, one." And it was the one that Mike referred to earlier. It was about an $8,000 transmission. And the member of Congress who was friendly to

this, to the program, said, wait a minute, you have cases of violence, right, that you stop, not just transfer of money. And the NSA guy had to say, all right, actually, no.

18:23:05

John Donvan:
Stewart Baker, we've been quoting for quite a few minutes here without letting you speak, so it's -- it's your turn.

Stewart Baker:
Yeah. I -- I have to say, there's a little confusion here. I hear Mike German saying, you know, all of these data collection programs are bad. And I think I hear Professor Cole saying, oh, no, those are all -- spying on us is fine if you're gathering data about travel reservations or border crossings. All of that data isn't the kind of spying on us that we're opposed to. We're opposed to this one program that relates to NSA.

And I think that suggests that they really don't have the courage of their convictions, that information that is available to third parties should be used for security purposes. That's the position that we are arguing here. And I think we've done a good job. On the question of whether NSA and its program responds to a very real problem, let's remember how they got started with this program.

18:24:07
In the months before 9/11, NSA was listening to communications in Yemen, and they heard calls from an al-Qaeda operative. What they didn't know is that the al-Qaeda operative was planning the hijacking in the United States. And those calls were coming from inside the United States, because they had no way to look inside the United States to see where these calls were coming from. If they had known months before the attack that somebody was inside the United States at that high rank within al-Qaeda, there would have been an all-points bulletin for that person. They would have found him, and probably the attack would not have occurred. When you have a failure like that, you ask, what can we do to make sure that never happens again? And this program responds in part to that concern. And I think that's a lesson that is written in blood for the national security agency.

18:25:07

John Donvan:
Michael German.

Michael German:
Again, the public record disputes that. The CIA did know he was in the United States. But the CIA wasn't talking to the NSA or the FBI or customs is a totally different issue than whether they needed to collect the information. There were people in our

intelligence community in both the CIA and NSA who knew they were in the United States.

Stewart Baker:
A few people here and there, but the NSA did not know because they had no tools to know it, to say, "Well, if somebody else had done their job perfectly, you wouldn't have needed this program," is to say, you know, "If the world were perfect, we wouldn't need counterterrorism."

John Donvan:
[inaudible]

Michael German:
But you have to fix the problem that exists, not create a new problem by gathering data you don't need.

[applause]

John Donvan:
I'm going to come to the audience for questions in just a moment. And, again, I want to remind you if you raise your hand, a microphone will be brought from the side aisle, just hang for a second till the microphone reaches you. And then we'd appreciate it if you could stand up, and tell us at least your first name.

18:26:03
And then to really shoot a question at these guys, and really make it really focused as a question. In fact, why don't we go to that since I've got some hands up already. Sir, why don't you -- right down in front [unintelligible] mike can be brought down here. I was thinking in the very center, thanks.

Male Speaker:
Hi, my name is Michael. Is there an alternative implementable replacement to these data collection programs to keep us safe?

David Cole:
I think there is. I think --

John Donvan:
David Cole.

David Cole:
-- the framers came up with an alternative. It's an alternative that we used for 200+ years. And the alternative says that you respect people's privacy until you have reason to believe that they're engaged in some sort of wrongdoing or that they have some sort

of foreign intelligence that you want to get. And the -- but the point is it's individualized suspicion, and once you develop that, then you can tap their phone, then you can search their homes, then you can invade their privacy.

18:27:06

What the Fourth Amendment was designed to stop was dragnet surveillance, general search warrants that gave the government the power to just pick up everybody's information in the hope that they'd find a bad guy. Yeah, it's quite possible that they'll find a bad guy if they pick up everybody's information, but the framers said, "That's not the way we want to strike the balance between liberty and security because that gives up all of our privacy in the hope that it'll make us more secure. And I -- so I think we should stick with the way we've been doing it for 200 years and not let technology and the Internet push us towards dragnet surveillance.

Richard Falkenrath:
We have --

John Donvan:
Richard Falkenrath.

Richard Falkenrath:
-- we have, in fact, stuck with that for information the Supreme Court deems personal privacy information. We just don't for this category of information which you think should be categorized but the rest of the legal system in the United States doesn't.

David Cole:
Well, but that's actually the problem so if that's --

Richard Falkenrath:
[inaudible] your standard still applies to content, right? It still requires particularized approval to get the content.

18:28:06

What we're talking about here is information which you or whoever have given to a third party, namely, a telecommunications provider, and that they have in their system to use for their purposes and, as Stewart explained, the government needs for its purposes from time to time. So you're confusing the discussion by suggesting they're the same. These are different categories of information. And while you disagree with how the Supreme Court has ruled this, the entire system is built around this distinction.

David Cole:
Well, two points on that. First of all --

John Donvan:
David Cole.

David Cole:
-- I'm not the only one who says that this information is -- gives all kinds of private information. Mike Hayden has said that it's more valuable than the content itself in terms of determining what someone's doing. That's number one. Number two, the Supreme Court has actually, in its most recent decision on whether the Fourth Amendment covers GPS monitoring of a car in public, said, "Absolutely, it does." And five justices said -- because it involved an invasion of a property right --

18:29:03

but five justices said, "Because collecting all that information, even though it's in public, about where you go --" they were collecting where this guy went 24/7 for a month -- and all nine justices said, "That's an invasion of privacy, that requires Fourth Amendment protection," rejecting the very position that Rich Falkenrath is putting forward, that, "Well, if it's in public, there is no expectation of privacy," or, "If you share it with a third party, there is no expectation of privacy." The reality is that everything we do today is shared with a third party. Every time you walk anywhere with your phone, you're telling the phone company where you are. Should the government be able to get that without any individualized suspicion?

Stewart Baker:
And I don't -- can I --

John Donvan:
Stewart Baker.

Stewart Baker:
-- a point where I think we do agree, of course the government should wherever possible be put to reasonable suspicion before it looks into individual activities. That is true even of the NSA program which is the one that you have chosen as the poster child for this issue.

18:30:07

No one is allowed to search this data without a reasonable articulable suspicion. So the question really boils down to "Are you allowed to collect it first and put it in the database?" And, look, the question I thought was an excellent one, "Why would you do that if there's an alternative?" and the problem is there's not a good alternative. The alternative would be to leave it with the companies and search it there when we have some reason to be concerned about that individual phone number, but the companies

get rid of that data on their own schedule. They've got no obligation to keep it, and they don't. Second, there are -- we got rid of Ma Bell. There is no one phone company you can go to search. No one computer system. So you would have to try to do this kind of analysis of who's talking to whom outside the United States and in -- you'd have to go jumping from system to system to system to system.

18:31:06

It's a nightmare. If you thought the healthcare.gov was bad, building this system would be worse.

John Donvan:
We -- we are in the question and answer section of this Intelligence Squared U.S. Debate. I'm John Donvan. We have four debaters, two against two, arguing it out over this motion: Spy on Me, I'd Rather be Safe. Let's go back to questions. Sir, right there. Orange necktie. Yeah, if you'll stand up, they'll find you with the microphone. I'm obviously tending to favor the middle, because you're right in front of my vision and the whole microphone thing would be a lot easier at the edges.

Stewart Baker:
Making it hard for the mic runner.

John Donvan:
Yeah. Yeah. I'm going to go to the edges next time.

Male Speaker:
[unintelligible]

Female Speaker:
You need a microphone.

John Donvan:
The radio wouldn't hear you.

Male Speaker:
All right. Sure. Hi, my name is Afar [spelled phonetically], and my question to the proponents of this motion is that the government is spying on me, you too, and everyone in this room, and if it were to know then did not expose these programs, how would I know and you would know that the government is spying on us, whether it's legal or illegal?

18:32:11

John Donvan:

Richard Falkenrath.

Richard Falkenrath:
It's a lot of different things, and so I think we're probably going to refer back to this telephone metadata question, and in that case, it's true that the scale of it was classified, but it was disclosed to every member of Congress in writing twice, 2009 and 2011, where the administration -- the Department of Justice -- by the way, the Obama Department of Justice -- wrote that this program, which we need you to reauthorize, which they did, broad bipartisan majorities, will entail the collection of substantially every telephone call record in the country. So they were told. Now whether --

John Donvan:
Congress knew.

Richard Falkenrath:
Yeah, so Congress --

John Donvan:
And they kept it secret.

Richard Falkenrath:
-- and if they didn't -- and they kept it secret -- it wasn't being hidden from them at that stage. You can make an argument about an earlier program up to 2006, but for that program in writing they were told.

18:33:03

John Donvan:
Response from the other side? You don't necessarily have to --

David Cole:
Again, when Ron Wyden asked James Clapper at a hearing, "Are you collecting data on millions of Americans?" he flatly said "no, we're not." That he's talking to Congress, he's talking on the record, he's talking to CSPAN, he's talking to the American people. They are lying to us.

Michael German:
And members of Congress, members in the House have complained that the House Intelligence Committee will not give them access to records. You know, the exceptive classification on these programs makes it so that only the member can see it, not the staff who actually have the time to work on these programs, to understand the legality, so it's not as easy as it looks.

John Donvan:

So, go ahead, yes?

Stewart Baker:
I was around for the creation of the legal structure around intelligence, and it was a remarkable achievement for the United States. No other country thought you could do intelligence under law. We set up a program that was designed to prevent the abuses that had occurred in the 60s and 70s, and by and large it has done it.

18:34:05

But everyone knows -- everyone here knows you can't do intelligence in the open because the people you're trying gather it on will be watching more closely than anyone else to figure out how to defeat it. At some point you have to say, I've got to trust somebody. In this case we are trusting 14 judges, two different administrations, committees headed by different parties over almost a decade. At some point, you have to say, yes, I would love it if I could know about this, but I realize that everything I know about Al Qaeda knows about, and I have to trust somebody. If I'm going to trust both parties and all three branches of government, that's probably as good as it's going to get.

Michael German:
And let me just challenge the idea that this is kept secret so that the terrorist doesn't know that they're doing this, because I worked and met a lot of terrorists working with them and every single of them and every single criminal I worked undercover against knew they were -- that they were a terrorist or a criminal.

18:35:05

[laughter]

So they knew that there was probable cause to believe that they were a terrorist and criminal, and yet they knew that the Fourth Amendment existed. So they don't worry about suspicion-less collection, because they know they can get caught up in reasonable suspicion collection, probably cause, proof beyond a reasonable doubt suspicion, right? So this was secret to keep it from us. So we wouldn't know we were being spied on.

David Cole:
I think you have to address the fact that Jim Sensenbrenner, the leading Republican on the judiciary committee who wrote section 215, he says "this program is beyond anything that I would have ever dreamed of authorizing." And how can that be if he was read into the program and -- is he lying to us?

John Donvan:

Okay. Right down in front.

Female Speaker:
I think one of the more compelling arguments against the proposition is that it's just not practical. There is -- there is billions of numbers being collected all the time. And both of y'all seem to have a very extensive experience in this field.

18:36:07

Do you find that it is actually impractical, that agents are being completely overwhelmed by the numbers they're seeing every day and not at the higher levels, but down, the folks who are actually doing the collection and [unintelligible]?

John Donvan:
Stewart Baker?

Stewart Baker:
I'll try that. There is always a risk that you will be overwhelmed by data. 90 percent of the data in the world was created in the last two years, apparently. I think that's about 40 percent my kids' Facebook postings.

[laughter]

But in fact, the tools for analyzing that are also pretty good. And no one at NSA said, we cannot keep up with this data. Once you've put it in a proper framework, they were only doing, after all, 300 identifier searches in a year. It was not a problem doing those searches. It was not a problem collecting and putting the data into a database.

18:37:00

There may be times when an ordinary agent says, "I've got too much data," but in this program and in the program I talked about earlier, with travel data, the computer systems allowed us to use it very effectively.

John Donvan:
I want to -- that was kind of Michael German's opening point, that there is too much. So I'd like to hear your response to Stewart's response to that.

Michael German:
Well, one of the major controversial programs was a similar program collecting internet data that ran. That was the whole hospital room confrontation with attorney general --

Male Speaker:
Ashcroft.

Michael German:
-- Ashcroft. I'm sorry. And they ended that program in 2011 because they found that it wasn't actually very effective. So for ten years, they collected our records, and it took them that long to decide they weren't actually very useful.

John Donvan:
Ma'am, you just had your hand up. Right behind you, sir.

Female Speaker:
Thank you. My name is Shelly. And I'd like to talk to the point -- ask the question about the point of what data mining means to our privacy and our safety.

18:38:10

I have to admit that whenever I hear a government person say, "Trust me, "I get very skeptical about what they're doing. We have a long history in this country --

John Donvan:
Okay. I'm going to stop you there because I would rather let them make the speeches. But your question is good, and when I -- and it feels like a big softball to this side. But -- but I think it's worth getting some more detail about the way in which -- that you -- you know, you proposed something that's not happening, the TV camera in the bedroom. But let's say that data mining is happening. And what are actually the risks to privacy, aside from the kind of creepy feeling that you described having, that it can be done? What are the actual risks in the implementation? And I'll let David Cole take that.

David Cole:
Well, the risks are that with all of the -- I mean, the same logic that gave them access to the phone records would give them access to your email records, to your internet records, to your credit card records, to your bank records, to your phone location data.

18:39:12

And the danger is you put all that information together, and they can determine everything about us. They can know more about us than our closest friends know, than our spouses know. And the only thing that -- if you give them all that data, then the only thing that's stopping them from doing that are these so-called backend safeguards which were routinely violated by the NSA and which we've -- we didn't have any opportunity to debate as to whether they were adequate or not because they were put in place entirely in secret.

John Donvan:
Richard Falkenrath.

Richard Falkenrath:
The "they" that you just described, "They can put all this together, they can understand --"

David Cole:
The government.

Richard Falkenrath:
Yeah. It sounds a lot more like Google than the government because -- and you have to take this -- this is actually a serious point. This is not the case that the government is tracking everything you do and can put it all together. And the government doesn't care what you're doing.

18:40:06

They're actually, though, in the last 10 years, with the explosion of social media and the explosion of terms of service agreement and informed consent that no one reads, is -- what you just described emerging in the private sector, with a legal basis being a document which no one can really read and give informed consent to; unlike the program we're talking about, which is subject to extreme safeguards, rooted in the Constitution, backed up by both chambers of Congress and by the judiciary. And so I think you've really got to shift your terms of your argument here. This isn't the '70s with the FBI running around at the behest of Richard Nixon probing into people's lives. This is a world where the government is tightly regulated and overseen in a way subject to law. And it's the private sector, if anything, which is emerging as the "they" in your scary scenario.

David Cole:
Well, the fact that the private sector may -- may threaten our privacy is not a justification to allow the government to invade our privacy, for two reasons.

18:41:06

One, we can establish limits on private sector. But two, for the reasons I suggested earlier, there are lots more reasons to be concerned about the government having access to this information than the private sector having it. And that's reflected in our Constitution, which constitutionally limits government access to data, does not constitutionally limit private access to data. There's a reason for that. And it's a good reason.

John Donvan:
I want to point out, tonight's debate is being broadcast worldwide on our website, iq2us.org and on fora.tv. It's also being seen on Arizona State on live stream. And I'm

just saying that because in the time we have left, if you're watching it and would like to join in the audience participation question, you can try sending us a Tweet on it. And if we can pick it up in time, our hash tag is "spy debate." And we'll try to work it into the debate. If you send that Tweet, the NSA will know that you have --

[laughter]

Male Speaker:
They already know.

John Donvan:
So think carefully. Another question, right up there.

18:42:05

Female Speaker:
Hi. My name is Kadeeja [spelled phonetically]. I was going to say, if the NSA wanted to be safer, why did they lie to Congress about spying on us?

John Donvan:
Stewart Baker.

Stewart Baker:
I'm --

John Donvan:
Well, really, the question is -- really, I think the question is, should we be troubled that the NSA is accused of having been dishonest?

Stewart Baker:
I don't want to defend what the DNI said there. He was, as far as I can tell, surprised by the question and made an error in his answer.

[laughter]

But, no, I'm sorry. How could he have said, I'm going to lie people after having gone out and said, "I want everybody to understand this program." That's -- it's quite clear that he had set up and agreed to provide this information to everyone. And so I don't think that we should be saying that there is a -- there's intentional lie being undertaken in that context.

18:43:09

John Donvan:

Other side want to respond? Michael German.

David Cole:
And it was an unintentional lie? At that time, nobody knew about this program. We didn't know. Edward Snowden hadn't stolen the information. He was asked, point blank --

Stewart Baker:
This information was provided to everybody in Congress.

David Cole:
Everybody in -- a letter was written that we -- you're assuming every member of Congress -- every member of Congress --

John Donvan:
You know, I want to move on because --

David Cole:
-- reads every letter that's sent to [unintelligible].

John Donvan:
I think the side argument on what he --

Male Speaker:
Let me just clarify.

John Donvan:
-- said will not help the audience vote on the motion so I'd like to move on.

Michael German:
But Senator Wyden did come out and say that he had given the question 24 hours in advance.

John Donvan:
Okay. Right up here. If you can stand, please. Thanks.

Female Speaker:
Hi. My name is Cassandra. I wanted to ask about the effect of the revelations of these programs on our foreign policy. Could you speak to that, please?

John Donvan:
That's another one where -- well, I'm not sure that that's relevant to the question of how we should feel about being spied on ourselves, so I'm going to pass on that question.

18:44:05

Male Speaker:
[unintelligible] I can take that.

John Donvan:
I know you can take it, but --

[laughter]

John Donvan:
Sir, right up there.

Male Speaker:
Hi. My name is Jamie. It seems to me the central issue here is a reasonable suspicion. So my question is, is the massive surveillance that is being on debate here necessary to ascertain whether someone is a reasonable suspicion or not?

Stewart Baker:
Let me try this one.

John Donvan:
Stewart Baker.

Stewart Baker:
There -- no one looks at these numbers without reasonable suspicion. That's the standard that is required by some of the safeguards, not all of them, but some of the safeguards that are already built into this program.

John Donvan:
And Stewart, just to clarify, so that means the data's available, but nobody actually goes and looks at it.

Stewart Baker:
Right.

John Donvan:
Okay.

Stewart Baker:
That's right. So that was done quite consciously because everyone at NSA and in the government believed that the right answer was not to look at data without some reason to believe that the person that you're looking at is engaged in suspicious activity.

18:45:06

The only difference between a standard law enforcement search and the searches we're talking about in the context of NSA is they gather the information first and put it in a database, but didn't search it without a reasonable suspicion. The reason that they gathered it first was because it was not practical to leave it where it was. They would not be able to do the searches in the time with the efficiency that they needed to use.

John Donvan:
Would someone like to respond?

Michael German:
So part --

John Donvan:
Michael German.

Michael German:
-- part of it is that the harm comes from the initial collection, right? If we know -- and there's studies to show this -- if we know we're under surveillance, our behavior changes, right? Every time that you're on Google and you hesitate before you put that search term in or you hesitate to go to that website that does damage to the fabric of our society, to the idea that there's a marketplace of ideas --

18:46:01

[applause]

-- so that original collection is a harm. But even with the limited number of searches, they go three hops. So it's the reasonable suspicious number but the people they called, the people they called, and the people they called. And then that -- it's like a big scoop that goes into this database, pulls out all those numbers which could rise into the millions --

Stewart Baker:
Pulls out 500 numbers. They put in 300, they brought out 500, and they gave 500 numbers to the FBI. They didn't bring out a great gob of data.

Michael German:
They said they go three hops out, so if you only talked to two people, perhaps five --

Stewart Baker:

No, they go to many places looking for suspicious numbers. When they find the suspicious numbers, they take it to the FBI. They only took 500 numbers to the FBI.

John Donvan:
I thought I saw a hand.

David Cole:
That doesn't say how many numbers they looked at. That just says how many numbers they --

[talking simultaneously]

Stewart Baker:
[inaudible] names attached, it was just --

Michael German:
The minimization standard says the numbers from the three hops go into the corporate store. The corporate store can be searched by anyone for any reason.

18:47:07

If there's -- the minimization limits aren't on the corporate store. So it's like a big scoop that gets it, puts it in the store, that data can be used for a myriad purposes.

John Donvan:
We have time for one more question, so make it good.

[laughter]

Female Speaker:
Hi, my name is Sue. And my question is for Mr. Baker. It seems at the heart of your argument is the sense of credible threat, that the public believe that there is a credible threat. But the government can't tell us what it is. They cannot reveal -- they can only say, "We've uncovered plots." They can't tell us what they are. As a journalist, I've had the privilege of talking with numerous people who do counterterrorism and journalists who cover that. And they've looked me in the eye, and they said, "The threat is real." And I believe that.

John Donvan:
So is your question, "Should we --"

Female Speaker:

But my question is in the wake of supposed WMDs in Iraq, why should the public believe the government?

18:48:05

Stewart Baker:
I think that's a fair question. And the real answer is you don't need to believe the government. Sure, the government has access to particular threats. But it doesn't take a security clearance to know that there are a lot of people who would like nothing better than to kill everybody in this auditorium and would be delighted to have done it. We live -- that's the world we live in, and the technology that we all enjoy has empowered them. You couldn't have pulled off 9/11 30 years earlier. What I'm really suggesting is that having empowered everyone, and increasingly empowered people on the other side of the world who hate us, to cause serious damage here, we need to let the government use the technical tools that are created by lower cost for storing data to offset the advantage that the terrorists have.

18:49:06

That's -- it seems to me you don't have to have a security clearance to have a commonsense appreciation of what the threat is and how empowered terrorists are these days.

John Donvan:
[unintelligible] you had a good long run, and we're going to wrap up. I want to give you 15 seconds for a last word. Michael German --

Michael German:
Sure.

John Donvan:
-- for 15 seconds if you can do it.

Land this thing.

[laughter]

Michael German:
So we can demand accountability from our intelligence agencies, and we need to because the only way they're going to be effective -- we didn't know how bad things were on September 10, 2001, were right? So what happened now is we have less knowledge of what the intelligence community is doing and how effective it's being.

That can't work. We have to have transparency. That's how we get effective government.

John Donvan:
And that concludes round two of this Intelligence Squared U.S. Debate where our motion is "Spy on me, I would rather be safe."

[applause]

And here's where we are. We are about to hear brief closing statements from each debater in turn. They will be two minutes, each.

18:50:05

And remember how you voted before the debate, we're going to have you vote again immediately after these closing statements. And the team whose numbers have changed the most in percentage point terms of your vote will be declared our winner. On to round three, closing statements. Our motion is "Spy on me, I'd rather be safe." And here to summarize his position against this motion, Michael German. He's senior policy counsel for the American Civil Liberties Union's Washington Legislative Office. Michael German, ladies and gentlemen.

[applause]

Michael German:
Thank you. Thank you very much for having me tonight, and thanks to Stewart and Richard for a great debate. Let me close by talking about this problem from a different standpoint. I'm hopefully they only person in this room who's actually been part of a terrorist conspiracy so I have a little bit of insight on what terrorists want. They want you to be afraid. They know they aren't powerful enough to overthrow a government or popular enough to win an election. So their only tool is to use horrible violence to try to provoke a government into taking measures that damages itself.

18:51:06

They know that when people are afraid they make bad decisions, they act irrationally, and their hope is that the government is going to overreact to the threat, right? They're going to go after communities of suspicion rather than focusing on individuals who are meaning harm. One of the interesting things I found working in terrorist groups: they always have a manifesto, right? They create a clandestine organization and the first thing they do is tell everybody in the world who they are. From an undercover perspective, that's bad policy, but the reason they do it is because they're trying to provoke grievance so that -- they want to let the government know who to go after so that they start to build real grievance, and that's what starts to undermine the

government, when it starts losing its legitimacy by doing things that violate its own values. That's why I think the founding fathers were so genius when they created a system that inoculated against this kind of reaction, right?

18:52:04

It made sure that the government was accountable to the people and limited in the power that it could use, particularly in violating the civil rights of Americans, and what they knew wasn't that that was going to be a weak form of government, but that that would be the strongest government on earth. We don't need to be afraid. We need to demand accountability and we don't need to sacrifice privacy, especially for the illusion of secrecy.

John Donvan:
Thank you, Michael German.

[applause]

Our motion is: Spy on Me, I'd Rather be Safe; and here to summarize his position supporting the motion, Richard Falkenrath, former Deputy Homeland Security Advisor. Ladies and gentlemen, Richard Falkenrath.

[applause]

Richard Falkenrath:
Thank you, John, and thank you, David and Michael, for an excellent discussion and debate. I hope the audience understands that neither Stewart nor I are in favor of an unfettered, unchecked executive authority to commit domestic spying. That's not what we're arguing here.

18:53:03

We understand that this is an incredibly difficult area of governance and requires tough oversight, the involvement of Congress, and the involvement of the judiciary. So please understand that's where we're coming from. There is another side to this, aside from the legitimate interest in personal privacy that we all have, and it's security. And this is, as I said in my opening, not abstract, and I'll end with a brief anecdote. I was Deputy Commissioner of Counterterrorism in New York City Police Department. We were part of the FBI joint terrorism task force. In September 2008, we learned of a case. We knew nothing about it until we were told as result of electronic surveillance there was an individual in Denver developing a bomb and intending to transport it back to New York City for the purpose of attacking the New York City subway around, he thought, September 14, 15, or 16. We found out about that because of his electronic communication with his bomb-making trainer in Pakistan.

He drove across the country, FBI surveillance team in Denver acquired him and began surveilling him in the course of his drive across the country with one to two kilograms of TATP explosive in his trunk.

18:54:09

We began an investigation of his contact, who he was in telephonic communication with. As a result of that, dozens of people he was in communication with were identified. Quickly, his two key co-conspirators, and then subject to much higher levels of intrusion -- of intrusive investigation. This was a real plot against the city of New York, where I was at the NYPD, and it was stopped not entirely, but in large measure because of the techniques we were talking about here tonight. This is not abstract. There is another side to this, and it something which is very, very valuable.

John Donvan:
Thank you, Richard Falkenrath.

[applause]

John Donvan:
Our motion: Spy on Me, I'd Rather be Safe; and here summarizing his position against this motion, David Cole, a professor at Georgetown University Law Center. Ladies and gentlemen, David Cole.

[applause]

David Cole:
Thank you. Technology has changed the calculus of surveillance in a dramatic way.

18:55:08

It used to be if the government wanted to find out everything about who you hung out with, what books you read, who you were talking to, what you thought, it was very difficult, very costly for it to do so, and that was a check on the government's ability to invade our privacy. That check has gone out the window because of the -- because of Al Gore and the internet. We now -- it's now possible to learn everything about us through this third party information which Richard Falkenrath says we shouldn't be concerned about at all. I think we need to be concerned about it. I think we can strike a proper balance between the technology that makes it possible for this kind of very, very broad surveillance and the need to find bad guys. But we can't do so if the programs are run in secret, if the NSA is lying to us about it, and if we haven't had an opportunity to have a democratic deliberation.

18:56:10

And when we don't have that democratic deliberation, it seems to me it's very likely that the security people are going to go overboard on the side of security. And when they're collecting texts, they're collecting data on every text that I send to my high school daughter when I go to pick her up from school, and she hasn't come out, and I say, "Where are you? I'm here. Where are you? I'm here. Where are you? I'm here." Why does the NSA need to know that information? The only reason that they have access to that information is because they did it in secret because if they had done it in public and told us they wanted to gather that information to keep us safe, I think we would have said no. And you should say no.

John Donvan:
Thank you, David Cole.

[applause]

Our motion, "Spy on me, I'd rather be safe," and here to summarize his position in support of this motion, Stewart Baker, the first assistant secretary for policy at the Department of Homeland Security. Ladies and gentlemen, Stewart Baker.

18:57:04

[applause]

Stewart Baker:
Thanks, John. You know, when I started as general counsel of the National Security Agency, Janet Reno, the attorney general, came out for a visit. And this was a high-stakes meeting. She was deeply skeptical about whether this spy agency could be trusted at all, whether it understood what the Fourth Amendment was. And we were walking through an operations center with her when the director stopped, looked at a corporal who was going over some intercepts, and he said to the corporal, "Stand up, sir." And "what do you do if you find a communication by an American?" that corporal plucked out of a mass of people doing the intercepts, said, "Sir, we segregate that. We cannot disseminate it unless there's foreign intelligence in it."

18:58:03

We must take the -- we must anonymize the data and destroy it if there's no intelligence in it," which was the rule. And I thought to myself, you know, the first rule of lawyering is don't ask a question if you don't know what the answer's going to be. But the director was absolutely sure that you could pick anybody out of that agency and ask him what the rules were. He would tell you and would be proud of the fact that he knew them and would obey them. That is the culture of the National Security Agency. If you give

them the rules, they will follow those rules. They have -- we have given them rules in this context. They are subject to lots of constraints. We cannot say, "All of this public, or we might as well not try to gather intelligence." We have to set rules, we have to count on people to enforce them, and then we have to count on the goodwill of our agencies to carry them out because that's our only hope of being able to do intelligence under law. I think we can do it.

18:59:11

John Donvan:
Thank you, Stewart Baker. And that concludes closing statements. And now it's time to learn which side you feel has argued the best here. We're going to ask you again to go to the keypad at your seat and press keys number one, two or three. Remember, the motion is this: Spy on me, I would rather be safe. If you agree with this team that's arguing for the motion, push number one. If you agree with their opponents, this team, push number two. And if you became or remain undecided, push number three. And you can ignore the other keys. They're not live. And if you make a mistake, just correct it, and the system will lock in your final result, and we're going to lock this out in about 15 seconds, and then we need about two minutes to calculate the results for you.

So while that's being done, one thing I want to say is I've been exchanging glances with our executive producer who sits in the front row. And the thumbs-up came up about halfway through.

19:00:07

I think this is one of the best debates that we've ever had in terms of not only the material that the teammates -- that the opponents and teammates brought to the table, but also the spirit in which this was conducted and the respect, and the -- our favorite word -- the intelligence of it. So I just want to invite a round of applause for all of them.

[applause]

I also -- I also want to congratulate everyone who asked a question, and that includes the questions that I passed on. There was nothing wrong with any of them. This is the kind of thing that really makes you think, and your brain starts going, and I think in fact a couple of the questions that I turned down in themselves would make excellent topics for debate. So everybody who put their hands up and those who got up to ask questions, I want to thank you as well for doing that.

[applause]

As we said at the beginning, we would love to have you tweet about this debate. You can use the Twitter handle at IQ2US. That's us. The hash tag is SpyDebate. Our next

debate will be in New York City on Wednesday, December 4, if you can get up there for that. And I happen to know that there are some of our New York audience members who came down for this debate.

19:01:10

So you've got to copy that and go up to New York. The topic on December 4 will be "Don't eat anything with a face."

[laughter]

For the motion, Dr. Neal Barnard, he is a clinical researcher who studies the effects of diet on health. Also for the motion, Gene Baur, he is president and cofounder of Farm Sanctuary. Time Magazine called him the "conscience of the food movement." Against the motion, Chris Masterjohn, who is a nutritional sciences researcher, and he's the aproponent of the Paleo Diet, and Joel Salatin, who is a third generation alternative farmer. A limited number of tickets are still available for that one on our website, www.IQ2US.org. The McCain Institute is holding another debate right here in the Burke Theater on Thursday, December 5. They are debating this question, "Drone wars, are we going too far?"

19:02:01

To reserve a ticket for that, go to their website, McCainInstitute.org. And for people who couldn't join our live audience, there are a lot of ways to catch these debates, going forward, at IQ2US.org and on FORA.TV, and the McCain Institute debates can be seen on their site as well. And we would love to have you listen to all of our debates on NPR stations across the country. We'll almost definitely be broadcast here in Washington on WAMU, so tune in when that happens, and you can listen to your applause. And we're hoping to make it back to Washington again next year, so go to our website for up-to-date information on that. And before I announce the final results, I want one more time to turn the lectern over to Ambassador Kurt Volker.

[applause]

Kurt Volker:
Well, first off, let me say that these are issues that are in the news every day, that you hear about them all the time, but I do think this was the most serious, informed, respectful, and insightful discussion of these issues that I've ever heard. And I want to hear do you agree with that?

19:03:04

[applause]

And one of the reasons that, that is true is because of the person who has not yet been thanked, wonderful moderator, John Donvan.

John Donvan:
Oh, thank you.

[applause]

Thank you very much.

Kurt Volker:
On behalf of the McCain Institute I want to say thank you, and we've loved this partnership with Intelligence Squared. And we look forward to seeing you, as John announced, here in this room December 5, 5:00, on "Drone policy, are we going too far?" John?

John Donvan:
Thank you, Kurt.

[applause]

All right, so I -- it's all in now. I have the results. Remember, we have you vote twice, once before the debate and once again after the debate. And the team whose numbers have moved the most in percentage point terms will be declared our winner. Our motion is this, "Spy on me, I would rather be safe." The initial vote, before hearing the arguments 26 percent of you agreed with this motion, 41 percent were against it, and 33 percent were undecided.

19:04:05

So those are the first results. Remember, you need to move the most in percentage point terms to win this game. Here is the second vote. The team arguing for the motion, their second vote is 29 percent. They went from 26 percent to 29 percent. That's a 3 percent increase. That's the number to beat. Let's see the team against the vote. They were 41 percent to start. They were 62 percent at the end.

[applause]

They clearly beat that 3 percent. They are our winner. Our congratulations to them. The motion "Spy on me, I'd rather be safe," the team arguing for that has lost. The team

arguing against it has won. Thank you from me, John Donvan, and Intelligence Squared U.S. We'll see you next time.

19:04:42