THE BROOKINGS INSTITUTION

A DEBATE ONE YEAR AFTER SNOWDEN:
THE FUTURE OF U.S. SURVEILLANCE AUTHORITIES

Washington, D.C.

Thursday, June 5, 2014

Moderator:

BENJAMIN WITTES
Senior Fellow, Governance Studies
The Brookings Institution

Panelists:

JAMEEL JAFFER
Deputy Legal Director and Director, Center for Democracy
American Civil Liberties Union

JULIAN SANCHEZ
Senior Fellow
Cato Institute

JOHN "CHRIS" INGLIS
Former Deputy Director
National Security Agency

CARRIE CORDERO
Director, National Security Studies
Georgetown Law

* * * * *

P R O C E E D I N G S

MR. WITTES: Thanks very much for coming. My name is Benjamin Wittes. I'm a senior fellow in the Governance Studies Program here at Brookings, and this is one year to the day after *The Guardian's* first disclosure of documents given to Glenn Greenwald and Laura Poitras by Edward Snowden. Snowden did not actually reveal himself for another few days, so it's not actually one year of Edward Snowden himself, but it is the beginning of the Snowden disclosures.

And over the last year, as you all know, there has been just a flood of debate and hair tearing and triumph and suggestions for reform and suggestions of prosecution and all sorts of things, and we decided that for this event what we wanted to do actually was to try to not look back and try to talk as little about Edward Snowden as possible and to look forward, rather, past this first year and discuss what needs to happen now. And so we wanted to do it in a debate format, and we wanted to involve a group of people who have been, over the past year, very high signal in a debate that has had a lot of noise relative to signal in all sides.

And so, the resolution is U.S. Surveillance Authorities Require Fundamental Reform, and I want to talk a little bit about the panels arguing for and against the resolution as well as describe a little bit the format that we're going to use because it is slightly irregular.

Arguing for the resolution are two of the voices in this debate on the what you might think of as the "anti-NSA" or the "pro-reform" side, the anti-surveillance side, who I think have been sort of consistently most rigorous and serious.

One is Jameel Jaffer who is with the ACLU, has been working on the national security side of ACLU litigation almost since the time of 9/11. Jameel is an energetic litigator who has gotten a huge amount of material released through FOIL

litigation, and he is a truly excellent advocate. Whether one agrees or disagrees with his point of view on any given issue, he's always a pleasure to engage.

And with him is Julian Sanchez of the Cato Institute. If you ever doubt that this subject is one that completely bends ideology, and if you think that there's a left and right to it, just remember the name Julian Sanchez because Julian is with the Cato Institute. He's a libertarian/conservative and very much allied with, in this discussion, with what most people think of as the left. Julian is one of the most technically sophisticated and interesting -- legally technically sophisticated and technically, technically sophisticated critics of the law and the administration's interpretations of it. So, that is the "pro" side.

Against the resolution, let's start with closer to me, Carrie Cordero. The public debate on this subject has very, very few people who have ever had the granular experience of actually practicing law in front of the FISA Court. A lot of people make a lot of representations about the FISA Court. Carrie is somebody who has actually stood in front of the FISA Court and argued things. Carrie was a Justice Department official in what became the National Security Division of the Justice Department before and after it became the National Security Division. She currently runs the Georgetown Law School's Masters in National Security Law Program.

And with her is John "Chris" Inglis, so there are a lot of people who think they understand what the NSA is, and what I say is if you haven't spent time talking to Chris Inglis about the NSA, you probably don't understand it as well as you think. Chris was the Deputy Director of NSA until earlier this year including in the sort of eight months prior to that when the Snowden revelations happened. He is not your image of a signals intelligence guy or a spy, and he's one of the most thoughtful and open-minded people in this debate, and it's actually one of the neat things about his having left government is

that he's now in a position to engage the sort of public side of the debate in his personal capacity in a way that he wasn't before.

The format of this is going to be, I hope elegant, but in any event simple. It's going to work like this. Rather than my telling people when their time is up and policing time, I have -- I didn't know this existed -- there is now a chess-clock app available for iPhones. Each side has 30 minutes. When one side is talking, the floor is theirs. Their clock is running. When they sit down or tell me, the other side has the floor and can hold it as long as they want. I will keep both sides loosely apprised of how much time they have remaining. By their request, we're going to do sort of -- at the beginning each side is going to take five minutes. Each person's going to take five minutes of their time to give a sort of brief opening, which I will give them a little bit of heads up about when they get to that five minutes.

After that -- that will take an hour -- after that hour we will take questions from the audience, which I will -- flag me if you want to pose a question, and we'll take the last 20 minutes for those questions.

With that I think we're starting with Jameel. Is that right?

MR. JAFFER: All right. Thank you for the invitation. Ben, Brookings, Happy Snowden Day to all of you. Over the last year we've learned a lot about government surveillance, certainly more than the government wanted us to know, and I think it's fair to say that this surveillance has turned out to be far more extensive and far more intrusive than most Americans imagined it could be.

We've learned that the NSA is collecting information about virtually every phone call made or received on U.S. telephone networks. When you pick up the phone, whether you're making a domestic call or an international call, the NSA is making a record of who you called, when you called them, and how long you spoke for. The

Agency is collecting more than five billion location-related records each day, records generated by mobile phones.

For a decade the Agency also collected Internet metadata in bulk. It kept track of every website you visited and everybody you emailed with. You've heard government officials say more than once that this kind of data is only metadata, but you shouldn't find that reassuring. If the government has a detailed record of where you've been, whom you've called, whom you've corresponded with, it can learn an incredible amount about your life.

It can learn whether you've been to psychiatrist, to Planned Parenthood, to a gay bar. It can draw a map of your political associations, your professional associations, your intimate associations. It can learn whether you spent nights with your spouse, and if you didn't, it can learn whom you spent those nights with. It can learn whom you met with and when and for how long and how many times. The government knows exactly how rich that data is, which is why it is so intent on collecting it.

Michael Hayden, the former NSA Chief acknowledged a few weeks ago that the government kills people based on metadata, and the government is collecting a lot more than metadata. In the course of monitoring 100,000 surveillance targets outside the U.S., the NSA collects huge volumes of American's international communications, and many of their domestic communications as well. It's scanning emails into and out of the country searching them for so-called selectors or keywords. It's broken into the communications link that connects Yahoo and Google's data centers. We learned just a few days ago that the NSA is collecting millions of photographs each day to feed into facial recognition programs.

Of all the NSA documents that have been revealed over the last year, I think one of the most revealing is a slide that describes one of the Agency's so-called

collection posture. The NSA, the slide says, must strive to "collect it all, process it all, know it all."

So why should it trouble us that the Agency wants to collect it all, and that the Agency is doing essentially that already? Well, at the risk of stating the obvious, surveillance on this scale invades the privacy of millions of innocent people. It used to be that the government would have some form of suspicion, even probable cause before it conducted intrusive surveillance. If it had reason to suspect that you were a foreign agent or engaged in criminal activity, at that point it might monitor your phone calls or monitor you email, but now the logic has been reversed. The basic principle at the heart of the Fourth Amendment has been reversed, and the government conducts surveillance to find out who it should think of as suspicious.

That kind of surveillance, mass surveillance, doesn't leave any room for privacy, and if it's left unchecked it will leave less and less room for dissent. Citizens who are constantly monitored by their government will hesitate before visiting controversial websites or joining controversial political groups or using search engines to find sensitive information about politics, health, or sexuality. They'll hesitate before participating in political demonstrations or attending political meetings for fear of the notations that might be made in some government database, and each of those hesitations might be inconsequential on its own.

What does it matter, you might ask, if some high school student hesitates before running a Google search for information about Al Qaeda or substance abuse or gay rights or the ACLU? But the accumulation of those small hesitations will change the way we relate to each other and to our government. It will make public debates and private conversations inhibited, and it will make our democracy less vital. It will make us less free, and the sad thing is that those small hesitations will be entirely justified

because the kind of information the NSA is collecting could very readily be abused.

It's already been abused by some NSA analysts who use their authority to secretly monitor their love interests, but the information could be abused on a much grander scale. Imagine how useful this kind of information would have been for someone like J. Edgar Hoover. Imagine how useful it would have been for him to have a map of American's associations with one another, to have a comprehensive record, for example, of whom Dr. King met with and when. Imagine how useful this kind of information might be to a future administration intent on identifying and ruining its political enemies. How confident are you that we won't have an administration like that in 5 years or 10 or 20?

MR. WITTES: That's five minutes.

MR. JAFFER: You're going to hear Chris and Carrie say that the NSA's employees are good people who respect the rule of law, and I'm sure that that's true of the vast majority of them. But you don't have to think the NSA is malevolent in order to conclude that it's unwise to concentrate so much information, so much power in its hands.

We should have a system that accounts for the possibility that information collected for one purpose will get used for another, for the possibility that information meant to remain in the government's hands will get accessed by others, and for the possibility that the people in charge tomorrow have less respect for the rule of law than they should. As Julian will explain, this is not the system we have right now.

MS. CORDERO: Thank you. There's no doubt that some reform of U.S. government surveillance activities is on the horizon. The real question is whether or not the Congress is going to adopt more limited reforms that are aimed towards addressing the shaken public confidence in the intelligence community or foundational, dramatic reforms that can potentially lead us down the path of degrading important national

security capabilities that currently keep the country safe. I would suggest that the better path is to focus on those specific reforms that can improve public confidence while not degrading important national security capabilities.

So, the driving question becomes what problem is it that we're actually trying to solve because some of the reforms that are currently on the table are wildly out of sync with the actual information that has been revealed. And it's also worth noting that there have been significant harms from the disclosures, including operational, economic, and political harms.

What has not been revealed is that there is any type of systematic, deliberate, strategic-level misuse or abuse of NSA's authorities, and what we also have learned is that there is actually a significant amount of oversight and accountability that exists over NSA's activities, and this involves oversight of all three branches of government. It involves federal judges who sit on the Foreign Intelligence Surveillance Court, inspectors general, compliance offices, and so when we want to think about what might be meaningful reform going forward, one area that we can focus on is ensuring that those oversight and accountability mechanisms continue to be well-funded, well-staffed, and are continually evaluated for their effectiveness. We also can focus on making sure that there's more information made publicly available regarding how those oversight mechanisms monitor what's going on.

I mention the harms briefly, and I do want to focus on them just for a few minutes. So, with respect to the operational harm that's been caused by these disclosures, the government has, not surprisingly, been somewhat circumspect regarding how damaging these leaks have been. But Secretary of State Kerry recently said that the leaks have made it harder for the United States to break up plots, harder to protect the nation. A Department of Defense report recently found that the scope of the

compromised knowledge related to U.S. intelligence capabilities is staggering.

On the economic front the U.S. technological industry and communications companies have really taken the brunt of much of the particularly international reaction to the disclosures, and this is unfortunate because much of that initial reaction was based on misreporting of facts and subsequent misunderstanding of the law, policies, and rules that govern NSA's activities. And so another area of reform that will be useful to focus on is enabling the corporate sector to have more information available to it regarding its compliance with government requests that it can communicate publicly and help the companies recover from the harm that they have incurred over the course of the last year.

Politically, domestically, the U.S. Congress, a number of members are under pressure from a variety of constituencies to implement serious of potentially dramatic reforms, but we risk our law making, our national security law making becoming overly politicized. The international community has really played politics with these leaks, and for just one example look at the recent Civil Liberties Committee report that came out of the European Parliament that drudges up old grievances that things like now put into jeopardy the existing information-sharing initiatives like the Terrace Finance Tracking program, the sharing of passenger travel data, and important economic frameworks like Safe Harbor.

So, those are all harms that we have seen incurred, again without any demonstration that the NSA had any type of systematic abuse or malfeasance on its part in terms of taking advantage of the significant authorities that they have.

A final point on one reform that does seem to be already being implemented, and that is the increasing focus on the part of the U.S. intelligence community to engage in risk management in determining what types of national security

collection should take place.

MR. WITTES: That's five minutes.

MS. CORDERO: Okay. Just one final thought. Lawmakers will really need to take into account -- and policymakers -- that risk management doesn't turn into risk aversion, and we can come back to those points later. Thank you.

MR. SANCHEZ: I want to thank Ben Wittes and Brookings again for hosting this important debate and echo Jameel in saying it's a privilege to be sharing a stage with Carrie and Chris who I know are thoughtful and dedicated public servants. If we absolutely must have a nigh-omniscient, planet-spanning, electronic panopticon, then Chris Inglis is the sort of person whose hands I want on the lever, but I don't think that's the right way to think about whether we ought to have such a system.

When James Madison was drawing up the blueprints for our constitutional order, he did not rely on George Washington's personal probity. He created a system of checks and balances, like simple enough to empower Lincoln but restricted enough to survive a Nixon. And what you're going to hear, what you've already started to hear, I think, is that that's what's we've done; that we have an array of checks in place that ensure that vast though the NSA's collection authorities are, the information is controlled and cannot be misused, and all three branches of government are overseeing the point of that authority.

But I don't think that is a defensible inference from the record we've seen. Even if you look at only the very small subset of disclosed programs that we actually have fairly detailed information about, often that's programs that are, in fact, overseen by the Foreign Surveillance Intelligence Court or FISC, which a lot of the most intrusive and broad programs aren't because they're conducted overseas under Executive Order 12333, but still, of course, having enormous capacity to draw in huge

quantities of U.S. personal communications as for example the MUSCULAR program which intercepted data from the links between deep-backup data centers of entities like Google and Yahoo did.

If you consider three of those programs; the 215 Telephony program, the 214 Internet Metadata Bulk Collection program in 2011, and then upstream collection meaning pulling information straight from the Internet backbone under FISA Act, Section 702, in each of those cases what we have found in opinions that have been disclosed from the FISA Court is a situation where the FISA Court had signed off on program that, in the first two cases for three years, in the latter case for at least a few months, functioned radically differently from what the FISA Court had been led to believe.

So, in the case of the Telephony metadata collection, the FISA Court learned that in fact the minimization procedures, the limitations on querying that database, the requirement that the data only be searched for numbers after a determination of reasonable suspicion that they were linked to a foreign terror group had not been made. In fact of the 17,000 some odd numbers that were being queried on a regular basis, only a couple of thousand had actually had that determination made.

With respect to the Internet metadata, they found that effectively the dissemination restrictions they placed on that that all these vast quantities of metadata that are supposed to used exclusively for counter-terrorism operations were not being adhered to.

Under Upstream, again, much more data was being collected, much more entirely domestic communications were being collected given the technical mechanisms being used than the FISA Court had been led to understand.

And you could say, well, that's the system working. See, they eventually, sometimes three years later after a change of personnel, were made aware of the

problem and fixed it. But I don't think that's a system working. I think that's an honor system. That's someone at the right time in a position to know making the decision to inform an oversight body with no real independent capacity to police implementation of these authorities itself as they've acknowledged. I don't think that's the kind of thing, the kind of result that eventually someone chose to acknowledge and to attack the problem, sometimes years later, should give us that much reassurance.

Now, they can say, but there were no willful and systematic abuses. No intentional misuses of authority for political reasons, and I think here it was Stephen Glass, the famous, fabulous of the *New Republic* who was able to fabricate stories despite an incredibly rigorous fact-checking system at that magazine they brought over from *New Yorker*. Why was he able to do that? Well, because they had a system that was very good at catching errors, catching mistakes. What it was not equipped to deal with was someone who was deliberately trying to game the system given their deep knowledge of how that system worked, and so it became much harder to detect his fabrications, and I think if we look at history what we find is the most serious abuses, the things that were known to be the kind of thing that would trigger oversight, in fact took place along with a series of countermeasures designed to evade detection. So, if you think of J. Edgar Hoover's June mail protocol, which caused potentially illegal surveillance material to be shunted not into FBI's central recordkeeping system but into his personal and confidential file. Blind memoranda were used to disseminate some of that information; that is unmarked, plain bond paper that showed no sign of its origin so if someone who shouldn't have it got hold of some data from FBI files, you couldn't trace it back.

And one really amusing case, former Congressman Carl Munt from the House Un-American Activities Committee sent a series of letters requesting FBI files on

named individuals invariably who wrote back saying files are confidential. We cannot share that information. But then a historian eventually wondered why did he keep asking? Turned out that denials, the refusals of that information, were always hand delivered by an FBI agent who came with a briefcase containing the files that had been requested. But if you looked at the record created for overseers, you would find no sign of willful abuse. It's willful abuse that you are least likely to detect, and even less likely to detect when you consider the vast scale of collection.

In the 1970's then Attorney General Ed Levi shut down a wiretap he had inadvertently discovered on the offices of the NAACP. It had been running since the 1940's. He said, well, is an indictment forthcoming? Found that, shut it down. The problem is that when collection is as broad as what the NSA is currently doing, you don't have that kind of red flag that is sent up because clearly a wiretap of the NAACP office seems suspicious and especially when it's running for that long. When collection is as broad as it is, is that emails of former President Bill Clinton are likely to end up in their files even if he hasn't been specifically targeted.

It becomes in practice almost impossible to detect abuse that is minimally sophisticated enough to evade countermeasures, so I think what we need to do is reduce the scale of collection and design a system that assumes that we're not going to detect abuse when it happens because one of the problems with abuse is that when it does happen the abuse itself will tend to undermine the mechanisms of correction.

MR. WITTES: Thanks. Chris?

MR. INGLIS: Thanks very much. I, too, appreciate the creation of the venue, and I, too, have enormous respect for the three panelists and Ben here present today. I also need to hasten to point out that I'm no longer in the employ of the National Security Agency, the Department of Defense or the U.S. government, so my remarks are

my own, and they're largely informed by my 28 years at the National Security Agency.

I'm going to start in a slightly different place and Jameel and Julian would have heard this before, but I think we need to reset to first principles and actual facts.

The first principles for us in this nation derive from the Constitution, and the Constitution is quite clear, both in the Preamble and the explanation of that Preamble that the government was established to not simply defend civil liberties, profoundly important, but also provide for the common defense. Right? Those are two great goods that live side by side and upon the consent of the government, the government is expected to devise and employ an array of mechanisms, instruments of national power, to essentially help achieve both of those.

When NSA persons take their oath of office they're not told it's just to the national security side. It's to both sides. It's to both the defense of civil liberties and to the defense of the nation's security despite the fact that our name happens to only encapsulate one of those two things.

I would say that we're also keenly aware, at the National Security Agency of the 10th Amendment which essentially says unless you've been explicitly granted an authority, you don't have it. Right? You cannot do that which you are not explicitly authorized to do. The President's directive in January of this year reiterated that, not for the first time, but clarified that to make that painfully clear to all powers.

And I think against the possibility that then you have a polarized choice here, either you don't conduct intelligence -- and I didn't hear Julian say that -- I heard Julian say thoughtfully, that perhaps what we need is intelligence proportionate to the need, right, to essentially effect security but in full respect of privacy. I think I can subscribe to that, and I think that's in fact what I perceive, what I understand, what I believe is the system that we've already laid in place.

To start, we've not reached the end of history. There are threats that abound, right. The Director of National Intelligence in his February open hearing to the Senate Select Committee on Intelligence said that in 50 years' time he's never seen an array, a diffusion of threats of the kind and scope that the United States faces at this time. That said, that doesn't justify an overwhelming overrun, right, an incursion into privacy. It doesn't justify that, so to Jameel's points I would say the following.

The surveillance that is conducted by the National Security Agency is not vast. It's not what you've heard. It's not in the case of each and every one of these capabilities that's been exposed applied to everything at every spot, corner of the world. So, for example, in the 215 metadata database we do not collect who that telephone number is associated with. It's just the telephone number. There's no association of that telephone number to some living person, organization, political persuasion. It is impossible based upon that knowledge alone to discern what that might be. Of course, you could enrich that. Of course, you could cheat. You could do other things, but that then depends upon the controls that are imposed upon NSA.

We have never kept track of every website that an American has visited, though we did at one time collect the equivalent of metadata in cyberspace for emails; a to, a from, the time that that would actually occur, but not the websites that people would visit, and we have no means to know political associations, sexual persuasion. That would be a gross infringement to privacy, a gross overrun of the things that we can and should do.

I would say that NSA personnel have two searing memories kind of in their -- kind of their fundamental component of their brain. The first is a "never again" mandate that was given to us not first on 9/11 but after World War II. That was when all these institutions were created. Never again a Pearl Harbor, never again that strategic

surprise, that searing memory was reinforced in 9/11, but the second searing memory and a very important and equally important searing memory is the memory of the Church-Pike Commissions in the late 1960s. And despite the fact that what Julian and Jameel described as abuses attributable to that, those abuses have not been played out at the National Security Agency in my time in the last 25 years. We are not the New Republic. We don't attempt to plagiarize or cheat. We attempt to chase national security in full deference, right, to the need to protect at the same time privacy and civil liberties.

My five minutes are just about up. I would love to either in the question and answer session or in a follow-on to describe in any level of detail that you would like how the 215 program works, how the 702 program works, how Upstream works, so that you might have some confidence in that.

If something's out of balance in this debate, it's not, I think, privacy and national security. I think we've worked very hard to achieve an appropriate balance to those two, not trading one for the other but trying to achieve both. It's the transparency. It's the consent of the governed that comes from a full knowledge of how those programs actually have been arrayed and the oversight and accountability that acts outside the hen house to ensure that those inside the hen house are in fact behaving as they should.

MR. WITTES: That's five minutes. We've got 19 minutes on this side, 16 1/2 on this side. Floor is yours, gentlemen.

MR. SANCHEZ: When you say the abuses (inaudible) played out again, I willing to believe that's the case. I think the structure may be dangerous whether or not that's occurred. I mean there are reasons to pursue nuclear disarmament even though World War III hasn't happened yet, but I also wonder if a year ago had someone said what about the possibility that someone without authorization and for purposes of their own, good or ill, could just abscond with tens of thousands or perhaps millions of the

Agency's most sensitive documents, and you wouldn't even actually necessarily be sure what had been taken. And I wonder whether a year ago your response would have been that's not possible. That certainly hasn't happened and couldn't have happened, and so why should we worry about that scenario?

MR. INGLIS: I would have said that that's not likely, but it is possible. All of us have computer systems, either at home or at work to which are recorded privileges by the people who use them. If you've got your own computer system, you give yourself full privilege to do whatever you want to do with the darn thing. If you run a company, right, you then have computer systems that have various roles; system administrators, line administrators, private individuals, and they're accorded various permissions to do things on that system.

Mr. Snowden was a system administrator. He had a broad permission to do exactly what he was doing which is to access the capabilities that NSA essentially has devised for application to foreign intelligence purposes, not to the pursuit of innocents or Americans, but to essentially access those capabilities and to post knowledge of those capabilities broadly within the system that our analysts use to figure out if I have a challenge to go after some threat to the nation, how do I pursue that? What capability might I employ? So, the possibility that someone might have absconded with that and dumped that on the kind of doorstep as it were was not beyond the pale, but we went to extraordinary lengths to essentially understand the nature of the capabilities, the kind of the trustworthiness of the people that came to work for us, and we had not across 70 years been disappointed. We had not found someone who had so egregiously betrayed their trust.

There had been a few cases, but what's different in the last 75 years is the speed at which that might happen given the speed at which these systems work. The

good news was that there are actually two sides of our system, much like there are in any computer system. The one side essentially is what you might call the administrative side, which essentially intentionally presents information to people so that they might understand something about capabilities, means, methods, meetings that are going to occur.

The other side is the production system where you literally acquire the material that is the stuff of your business. You control that material. You make that material available to analysts, and you produce and disseminate that. You have access to the former, not to the latter. That's why you've not seen material of that sort.

MS. CORDERO: Just to add briefly to that, as well, what's interesting is that the point that you just made, Julian, really hasn't been sort of the central part of the debate of the last year. The discussion really hasn't been, and frankly I wish that it would have been, more about the fact how was it that he was able to walk out with this information? Are there more controls that are needed on the information that the government retains? What were the factors that went into his original security clearance grant? Things like that that really would be reforms and very valid questions responsive to what actually has occurred in the last year.

Instead what we seem to be hearing is, I think, in both Jameel and Julian's opening remarks is about half a dozen references to J. Edgar Hoover, which really bears no relation to the intelligence community that I certainly worked with for over a decade.

And instead what has happened with the public debate and particularly some of the legislative reforms that are currently pending before Congress is really a push towards scaling back our national security surveillance laws in a way that go back to the pre-9/11 era, so there are proposals that are currently on the table that it would make

it harder to get records again, basic records and investigation that would again change the calibration between going back to the days where it was harder to obtain records in a terrorism investigation than it was in an every-day drug investigation. So, it's interesting that those the proposals that are currently on the table, so many of them would dramatically scale back intelligence capabilities and not particularly be responsive to some of the problems that have actually emerged.

MR. JAFFER: I have a few sort of disconnected points. Chris, you used the phrase "not likely but possible." I think that was your phrase when Julian said "if I'd asked you a year ago about the possibility of a Snowden, you would have said not likely but possible," and I think that's probably a fair description of a lot of the abuses that I, at least, laid out. I mean they're not likely to happen, but it's possible that they'll happen, and over a sufficient amount of time it becomes more and more possible, and you approach certainty, and if you look at our own history, right, the history of this country, the history of other democracies, you can see that these powers have been abused in the past, and they were abused even when the powers were much narrower than they are now and the technology was a lot less powerful than it is now. And the argument that I was trying to make in my opening was simply that you need to take into account the possibility of that kind of abuse.

And something else you said, Chris, I think is related to this. You said, "we don't connect," and I'm sorry if I get your exact words wrong, but we don't connect the numbers to the names, right, when you collect the phone numbers that people dial, right. People pick up the phone. They make a phone call. The NSA has in its database the numbers that were dialed, the length of time of the call, the time the call was made. You don't connect that to the names.

First of all, it's very easy to connect it to the names, but even if you

don't connect to the names, there's a possibility that somebody else will connect it to the names. And it seems naive to me to set out this kind of system, to create this kind of system, on the theory that right now we're not making these connections when it's so easy for you or for someone else or the next guy to make those connections. And you have to create a system that takes into account the possibility of abuse.

I just want to address one other thing that you said, Chris. You credited Julian for acknowledging that the government has a legitimate interest in gathering intelligence, and I just want to make clear that I also believe that the government has a legitimate interest in gathering intelligence, and the hard question is the question of proportionality, but on that particular question I think one useful data point is our experience with the Call Records program because when the NSA went to the FISA Court to ask the Court to approve the Call Records program in 2006 and again periodically after 2006, it used this phrase that you can find yourselves in the documents that have been released by the FISA Court and by the government over the last few months. It used the phrase "essential," essential to the national security. This is an essential tool, and they use it over and over and over again. That phrase appears over and over again in the government's documents.

Since the program was disclosed, over the last year, the President's review group has concluded that the program is unnecessary. The Privacy and Civil Liberties Oversight Board has concluded that the program is unnecessary. The President himself has concluded that the program is unnecessary, so I think that we've already seen that programs that the government at one point said were crucial to the national security, were crucial to the common defense, are in fact not crucial at all to the common defense, and they persisted because of the secrecy, because of the unlawful secrecy that surrounded the programs.

MR. SANCHEZ: A couple quick points since Carrie says --

MR. INGLIS: Hey Julian, could I respond to Jameel --

MR. SANCHEZ: Sure.

MR. INGLIS: -- and then I promise I'll get to you. So, I think I agree with your first point, but your second point I'd like to challenge you in that regard. I'd like to read from a posting from the (inaudible) distinguished service of law professor, Professor Geoffrey Stone who's on the President's Review Group, and he says in this posting on the 31st of March "that when I accepted the appointment to be on the President's Review Group, to say that I was skeptical about the NSA is, in truth, an understatement. I came away from my work on the Review Group with a view that NSA that I found was quite surprising. Not only did I find that NSA helped thwart numerous terrorist plots against the United States and its allies since 9/11, but also found that as an organization, operates with a high degree of integrity and deep commitment to the rule of law. We found no evidence that NSA had knowingly or intentionally engaged in unlawful, unauthorized activity. To the contrary, it had put in place carefully crafted internal procedures to ensure that it operated within the bounds of its lawful authority. I hasten to point out that at end," he says, "that NSA deserves the respect and admiration of the American people, but it should never ever be trusted."

And how do I square that circle? I square that circle because he essentially makes the case that we as a democracy, as a people, are inherently mistrustful of the government. I can actually live with that because I am an American too. I can live with the fact that we can extend these authorities to an NSA given the need to prosecute national security to inform the instruments of national power, but we must be ruthless in the imposition of controls, oversight on top of that.

I take the point that these could be abused. That's always been a

"could." That's always been a possibility in the discussion of the last year. The fact that a single individual can walk away with a mass of material as Mr. Snowden did doesn't mean that a single individual inside NSA can affect the repeated activities that are necessary to essentially violate these rules. There's two-person control. There's oversight. There's accountability.

Let's take the 10 instances that you spoke about, Jameel, earlier of individuals at NSA who have been found to intentionally misuse the SIGINT system. The majority of those individuals across a 12-year period were in fact using the system that's available overseas, right, to essentially target foreign persons, and the majority of them, in fact, were trying to find out whether this person that they had a relationship with was true to them, had another person, another kind of friend, whatever that might be. That's why it was called by the press "Lovint," not by NSA.

By NSA it was called a crime, right, and despite the fact that this was rent upon innocent foreigners, NSA stepped in in each case, caught this literally within hours in each case, stepped in, removed the authority of that individual to use to SIGINT system any more. In the case of the military personnel, they were reduced in grade and there was a financial penalty. They all lost their clearance. None of them work for the National Security Agency any more. That's a big, big deal, but compare that against the tens of thousands of analysts who similarly had an opportunity to do something wrong. (A), the 10 who did who did were caught. They were caught quickly. They were dealt with severely even though it was innocent foreigners who were at prey, and (B), there were tens of thousands of those who did not. So, I take the point that there must be imposed controls, accountability on the system. I would say that that's actually worked quite well for us over the last dozen years and across my 25 years.

MR. JAFFER: If it works so well, then why is it that only after the

programs were disclosed did we learn that the programs were unnecessary? That the call records, why was it only after the program was disclosed that the government conceded that the program was unnecessary?

MR. INGLIS: The programs have not been declared as unnecessary. The President said that what he wants is a different implementation of that program to increase the confidence of the American public in those programs. Hold the data in a different place, but make the data available to the National Security Agency or the --

MR. JAFFER: The National Security Agency is not collecting call records in bulk. That's a huge shift.

MR. INGLIS: It's a huge difference in implementation, but at the end of the day that data is still available. It is still queryable by the National Security Agency through a different means, but essentially affects greater confidence that it won't be abused in the future, having declared that it hasn't been abused in the past. There have been compliance incidents. I'm happy to talk about those, but it has not been abused in the past. Geoffrey Stone says that. The President says that, but there is the possibility as you suggested in any program where exquisite, extraordinary authority is extended to an organization, a future abuse. And what the President says is we need to hedge against that. We should never allow a temptation, however great, in the future to allow us to make that mistake. And so what the President has said is I want a different implementation that gives me greater confidence for the same program.

MR. SANCHEZ: I don't think anyone is suggesting that it would be wrong for the NSA or any agency to get specific records (inaudible) application pursuant to a court order. I think it's a -- I mean the difference in means here is the critical difference, but I want to respond to bits of both Chris and Carrie here.

Carrie says, you know, yeah, it's important to talk about the potential for

this kind of exfiltration. You should be having a technical debate about how to improve security measures, make sure there's not another Snowden who perhaps did not helpfully reveal himself to the *The Guardian*, and so that help us track his improper exfiltration. One component of security though is the nature of what you're trying to protect. What is adequate security for your home or your piggy bank may not be adequate security for Ft. Knox, which is why security experts always encourage sites not to keep more personal information than is necessary.

The more information, especially information totally extraneous to a specific security investigation that is centralized in one database, the more attractive a target that becomes for an attacker and the more catastrophic the potential consequences in the event of a successful breach.

So, that's one kind of safeguard against attack, but of course that doesn't protect against the non-rogue attack, the abuse that comes from the top. And I think we need to think more realistically about what that looks like when it happens. We say we haven't found willful abuse. There's never going to be a memo in which Michael Rogers says "Ha, ha, ha. Now at last we turn the panoptic on inward and crush democracy."

If you look at what historical abuses look like, very often in their inception involved collection programs that were initiated for legitimate or at least legitimate foreign intelligence and national security purposes. (Inaudible) was initially launched on the premise that there was infiltration by Soviet agents, which continued despite the relative absence of the finding of that. Often intelligence gathered for absolutely legitimate wiretaps to look for foreign corruption made their way into the hands of the White House and were used as political intelligence to give the President an illegitimate advantage in negotiation with Congress.

And if we look at some of the disclosures more recently we see, I think,

the trajectory for how something similar would occur in the future. It wouldn't be let us crush, occupy. It would be something like a document that was disclosed by the (inaudible) discussing how to discredit radicalizers. So, it talked about -- I know they can't confirm this one -- but a group of English-speaking persons outside the U.S., one of whom was a U.S. person, and who were not affiliated with violent groups or not committing any crime, but who it was believed were stirring up anti-U.S. sentiment justifying Jihad and needed to be discredited, and found that they could be discredited by among other things circulating derogatory information about how they used the Internet to look at pornography, to pick up sexual partners in ways that were out of line with their self-professed image of devout Muslims.

That's the kind of information that you might reasonably collect for foreign intelligence purposes, but is shading into the kind of conduct that reminds one of the (inaudible) Program where in effect, surveillance is being used as a tool to essentially smear people on the basis of ugly and offensive but non-criminal speech. I think that's what, if there is abuse in the future, it will look like, not Emperor or Palpatine cackling about absolute power.

MS. CORDERO: So, let me take a minute to step away for a minute from sort of the fears of the way things might work and talk for a few minutes about how it actually does work.

With respect to the Telephone metadata programs, this is what you've heard called the 215 program, which now the President has made some changes to including now that the FISA Court is going to approve actual -- the seed numbers that get queried into the records database. But that 215 program, before the President even made some of the recent changes of the last few months was quite narrowly tailored, so original information was collected, but then the way that the controls were implanted was

that only a certain very small number, about 22 people at NSA, were able to have access to that information. They had to meet a legal standard, reasonable articulable suspicion that the number that they were going to query into the database was connected to terrorism. Then after they did that and it went through supervisory approvals, oversight personnel at the Department of Justice reviewed determinations and conducted oversight, and the intelligence committees of Congress were aware of how this was being conducted all along. So, it's not that the program sort of had all this possibility for abuse and misuse, it actually was a specifically-targeted program and implemented in a very specific way.

On the 702 program, which is another one that you've heard described, which is a collection program that occurs under the FISA Amendments Act of 2008 and collects contents, so this is actually content of communications that is of persons who are outside the United States for foreign intelligence purposes.

The Department of Justice and the Office of the Director of National Intelligence conduct very granular, onsite, detailed review of how that authority is implemented by NSA. So, it's not NSA that's just sort of out working on its own, even though it does have its own internal compliance mechanisms, there's outside Executive Branch oversight by DOJ and DNI. There's FISA Court oversight that approves how the targeting takes place, how the information is handled, all of the rules and procedures that are handled, and then much of this information is reported and detailed to the Congressional oversight committees.

MR. INGLIS: And Julian, I agree with your point that the collection of mass quantities of gratuitous information is a danger, not so much from the possibility of abuse, but there is a danger there, but from the possibility that it just might be through inadvertent inaction or just spillage, incur some great damage to the parties whose

information is exposed through that. I think that's why, right, the President in his directive, his second directive, Presidential Directive 28 said that we're going to necessarily kind of clarify the rules for bulk collection; that there must the rules -- I'll kind of put my own paraphrase into this -- that equate to necessity and proportionality. There must be some bona fide necessity to collect the information, and it should be describable. First Amendment freedoms are protected in that regard, and it must be that it's in proportion, right, to that need. It can't be gratuitous, and it can't be simply because I want it all, all the time for all purposes.

MS. CORDERO: One additional point on the President's initiative. So, there have been policy directives. The President issued a new order in January that does place additional limits on the collection. That is completely within the President's authority and is appropriate and so forth.

Where I think this debate over the last year is now taking a turn is now the President can make those determinations, and if it determines that those policy decisions are having an adverse impact on national security and he needs to adjust them, he currently has the flexibility to do that.

The problem with some of the legislative proposals that are currently on the table is that they will outlaw certain activity, and it will be in law if bulk collection, for example, is outlawed, can't be conducted under the FISA statute. And that's where we risk the potential to create an environment that nobody in the legal community or the national security community wants to revisit, which is the environment that we faced in the pre-9/11 days and right after where the law, the statutes, had become so outdated with respect to the way the technology occurred and the threats that we were facing that the Executive needed to act on Executive authority alone. And unfortunately some of the proposals that are currently on the table risk putting us down that path in the years to

come.

MR. SANCHEZ: Can I just pose the question of risk. If -- and again don't want to confirm anything -- but if it were the case the NSA were recording nearly every cell phone conversation that took place in the Bahamas, would that meet your test for proportional, unlimited collection?

MR. INGLIS: All the collection that we do, again, remember the 10th Amendment? You do, I know, but we remember it, too, has to actually have some purpose up front. It has to have some delegated authority. It has to have some purpose in mind, and so we need to make the case whether it's done under Executive Order 12333 which essentially gives us broad permission to do things overseas or under Court supervision when that has a domestic nexus, kind of when the collection event might occur, again, for foreign intelligence purposes on U.S. infrastructure, has to have some foreign intelligence purpose in mind, and you need to be able to describe that. There needs to be a reasonable foreign intelligence purpose, and those standards become much higher based upon some particular authority that actually imposes higher standards whether that's 215 or FISA. And so, if hypothetically we were to do such a thing there would have to be some bona fide foreign intelligence purpose in mind, and it would have to be necessary and proportionate to that foreign intelligence purpose.

MR. JAFFER: Could you imagine a foreign intelligence purpose that would justify that kind of collection?

MR. INGLIS: Hypothetically? No.

MR. JAFFER: You know, I wonder whether there's a certain amount of talking past each other here because I hear both Carrie and Chris going back repeatedly to this question of compliance and making the argument that the NSA is complying, that the government more generally is complying with the laws that Congress has passed,

and there's a debate to be had about the extent to which that's true, but even if you accept that it's true, my larger concern is with what they're complying with, right.

In my view a large part of the scandal here is what Congress has legalized, and when I say that we need fundamental surveillance reform that has to be directed at some of the statutes that Congress has passed. Congress has authorized far more surveillance than is consistent with the Constitution and far more surveillance than is wise in a country that cares about privacy and the freedoms of speech and association.

And when I hear Carrie and I think especially Chris keep going back to this question of the integrity of people at the NSA and the question of whether they comply or not with the instructions that they're given by Congress, for the most part I don't disagree with that. The question to me isn't so much whether people at the NSA are good people or not. The question is whether the rules that Congress has given them are the right set of rules, and if that set of rules allows the NSA to collect information about every phone call made in the United States or every email sent to the United States or allows the NSA to essentially scan through every text-based communication going into and out of the country, I just don't see how that could possibly be proportional to the government's legitimate, and I think we all agree that it's legitimate, the government's legitimate interest in tracking, for example, suspected terrorists.

MR. WITTES: So, we have almost exactly five and a half minutes on both sides left. People have been remarkably even, so I just wanted to give you guys a heads up that that's where we are. Floor is yours.

MR. INGLIS: I would say that I agree. I'm with the bottom-line premise that Jameel's put on the table which is that compliance is no excuse for a bad law, bad policy. I don't think that's where we are. I think that the laws, the policies, the orders that have been granted to NSA have demonstrated necessity. They are, in fact, applied

proportionately, and we've actually then kind of discerned through many and varied oversight instruments that there have been no willful strategic abuses. There have been those 10 individuals I referred to. They've been dealt with, but there hasn't been any systematic abuses in that regard, and NSA isn't alone. I'm expected to report to that. We should be expected to exercise that degree of due diligence and conscience, but there are manifest external oversight bodies. There are many, many people at NSA with clipboards, right, and darn few with hands on keyboards and that's okay, right. If that's the price for these delegated authorities, I'm fine with that.

And let me just read something else from Geoffrey Stone's note of 31 March. He says that "I was only following orders is not an excuse, but in no instance was the NSA implementing a program that was so clearly illegal or unconstitutional it would have been justified in refusing to perform the functions assigned by Congress, the President, the Judiciary."

There are many legal scholars who have said I question whether the 215 program is legally justified or whether some other things are legally justified, but in fact it was the combined efforts, right, of the Congress in essentially passing the law and various specific members of Congress understanding the detailed implementation, understanding of the interpretation of that law; both of the intelligence oversight committees, the Executive Branch in implementing that law, and 37 federal judges essentially approving the implantation of that law, and that's across multiple parties, multiple administrations, multiple ideologies.

So, if you're at NSA and you believe that there's a national security purpose, -- we do -- if it's necessary and proportionate to that need and you've seen essentially that whole of government pass judgment on that, I have a really hard time understanding how we could possibly say it's unconstitutional.

MR. JAFFER: Just on the FISA Court point, I think it's important for people to understand how the FISA Court operates here. It's true that the FISA Court approved this program. The FISA Court approved it without an opinion. It didn't think it was a significant enough request for authority to justify an opinion in 2006 when it was asked to bring this program under Section 215. It didn't address some of the main constitutional arguments against the program until the program was disclosed, and in fact, the first opinion to be written by the FISA Court about this program was written in 2013 after the program was disclosed.

The FISA Court is a court that meets in secret and hears only from the government. It doesn't hear arguments from, for example, civil liberties groups who might have an interest in pointing out the constitutional arguments on the other side, and I think that if you look at the FISA Court's opinions on this particular instance and their rulings on this particular program, you see over and over again that the Court is kind of blindsided a year or two years after an issue is first raised with the constitutional arguments on the other side because the government's lawyers who appear before the FISA Court, while I'm sure they're conscientious lawyers and they're trying to present the arguments in a way that's fair, at the end of the day the government's lawyers are representing the government, and they're there in order to get the government's programs approved. And the FISA Court is hovelled by the absence of any advocate on the other side, and I think that it's a very good thing that among the reforms that some legislators have proposed a reform to the FISA Court.

MS. CORDERO: With respect to the FISA Court's activities, so I know we're close on time, so a few court's points very briefly. First, there have been proposals to add institutional advocates and sort of another side to the FISA Court proceedings. The former presiding judge of the FISA Court himself has said that those proposals would

be both unnecessary and unproductive and really get -- that's his language, unnecessary and unproductive. In other words, they really would get in the way of the FISA Court doing its business.

The FISA Court is made up of regular federal District Court judges, who hear wiretap applications all the time and they don't have another side that's present when they hear those in their District Court capacity. And so the judges are quite capable of making decisions on their own.

Another point, just going back to something that Jameel said earlier, is that with respect to the broader conversation about whether the laws that Congress has passes are appropriate, many of the issues that are currently on the table pertain to sort of what our Fourth Amendment rights are and whether we have an expectation of privacy and whether something that's called the Third Party Doctrine, which is that when we give records to a company, we don't have an expectation of privacy in them. Some of the current proposals want to change that construct on the national security side. The problem with that is that's how law enforcement works every single day is on these principles, these historic Supreme Court principles regarding our expectation of privacy. And so we need to keep in mind that this conversation is really not just about the national security space. When we get into the Constitutional precedents and the Supreme Court precedents, there really will be a meaningful impact on the law enforcement side. And what we don't want to do is end up again in a situation where the national security authorities are much more stringent, much more difficult to work and to protect the country than in regular law enforcement construct.

MR. INGLIS: So to the point of whether an advocate at the Court representing kind of perhaps, you know, the loyal opposition would be useful, I personally think that would be, not because it's been missing. I think the conscience of these

federal judges, they're no wilting flowers, right, they're quite serious about the rule of law. It doesn't matter whether they're kind of behind chambers acting as a grand jury would in secret or whether they're kind of outside kind of being held accountable in public, they're very serious about their roles, their responsibilities. But having someone there who could effectively ensure that there's a full, rigorous discussion that's then documentable for purposes of the precedent that it established, I think that's a good idea.

MR. WITTES: We have 1 minute left on this side, 3-1/2 minutes left on this side.

MR. SANCHEZ: So I think one thing that should be mentioned here is that while there are many parallels between the criminal and intelligence investigative systems, there are a lot of ways in which the intelligence powers are broader, even if it's superficially similar, but that also secrecy changes everything about those systems and radically dilutes the functioning of the checks that are in place. So, of course, yes, wiretap orders under Title III as under FISA are heard ex parte without an opposing side present. But the fact that on the criminal side those orders are granted with the knowledge that they must be disclosed to the target and with the understanding that the point of the tap is to generate an indictment that will result in a trial, that will result in discovery obligations to the defense, that will generally result in challenges that create new Fourth Amendment law most of the time -- that's where our new Fourth Amendment law usually comes from -- alters the situation.

The fact that judges know that their opinions will be public will be the subject of law review articles, might produce a scathing response from an Appellant Court. These are all things that condition the behavior of attorneys, the behavior of judges, and certainly the behavior of overseers in Congress who manifestly have reacted differently to these programs now that the public is conscious of them.

And secrecy is also a problem in terms of identifying whether or not, again, abuses have occurred. Because when you talk about the problems that have been encountered to date, they sound perhaps not as trivial or more trivial. You know, problems with minimization rules. Minimization rules weren't followed. There was not the restricted sort of dissemination that the FISA Court had implemented. The thing that's important to understand about that is that once those boundaries are crossed, once the formal rules which are in place because the use of the data is secret, once the controls on how that data flows have been disregarded, then your ability to say with any confidence how that data is being used for good or ill diminishes radically. And the more data you have, the more in each instance you need to ask whether that boundary crossing has resulted in an information leak too tempting for someone on the receiving end to pass up.

MR. WITTES: You guys have a minute left.

MS. CORDERO: Thirty seconds. So in my 30 seconds I'll say that with respect to sort of things happening in secret, the deal that was struck in 1978, after the Church and Pike committee said, that Chris mentioned earlier, is that we would have closed intelligence committees that do get to review what the intelligence community does in secret and that we would have a Foreign Intelligence Surveillance Court that would operate in secret. And the balance was that, therefore, all three branches of government were involved, but we could still have that oversight in the context of being able to protect the nation through national security activities.

If we want to change that whole system, then that's sort of a new debate that needs to occur. But what we can't do is sort of blame NSA for operating within the system that the government had set up for it for the last 30+ years.

MR. JAFFER: I think we want to change the whole system. And, you

know, are, I think, once again going back to this question of blaming the NSA. I'm not blaming the NSA, you know. I'm not interested in whether the NSA's to blame or not. The question isn't whether the NSA is to blame, but whether the system we have in place is the right system given the far greater power that the government has now than it did in 1978. In 1978, when the government appears before the FISA Court it appeared asking for an individualized warrant -- or an individualized authorization based on probable cause to wiretap a specific person or a specific organization's phone, and that's not what's going on now. Now when the government goes before the FISA Court they're often asking for authority to engage in the kinds of bulk programs, the dragnet programs that we've been talking about, and that's a very different enterprise and it requires a very different system of checks and balances.

MR. WITTES: So both --

MR. INGLIS: Can I have 20 seconds?

MR. WITTES: Please.

MR. INGLIS: Two things. I do challenge the premise that this is a system operating in secrecy. The question is secret from whom? Right? If it's secret from everyone except the implementing agency, NSA, I challenge that absolutely. The granting of these authorities involve two or three branches. If it's Executive Order 12333 at least two branches are involved. For the programs we've been talking most about, 215 and 702, three branches are involved in the granting of these explicit privileges.

And in the implementation? Three branches are involved in the oversight and accountability. You can't get away with murder or kind of cheating on what communications you're going to go after.

And with respect to the issue of kind of in 1978 you had to have probable cause every time you targeted something, today every time you target, you go before the

Court and you attempt to target the communication of a U.S. person anywhere in the world, you need probable cause. And that standard has been tightened since 1978, not loosened.

MR. WITTES: Julian, do you want to take the last word?

MR. SANCHEZ: Well, what (inaudible) is that oversight can --

MR. WITTES: But before you do, people in the audience who want questions, flag me and while Julian is talking I will direct the microphone your way.

MR. SANCHEZ: I mean, I think the fundamental problem here is that we have a system of oversight designed for a much targeted [*sic*] and a much smaller scale collection. You know, it may be possible to oversee 10 people and very hard to oversee 10,000. Oversight does not scale very well. And so we may need to confront the possibility that something that was manageable under a much more targeted model is not realistically overseeable at the vast scale to which NSA collection has grown.

And then the question we need to ask is if the scale is so tremendous that oversight becomes more sort of decorative than meaningful, that it becomes not really possible in any kind of granular way to really oversee the vast array of incredibly complex programs, a problem that was cited again and again in some of these documents, the problem was too vast and too complex for anyone even within NSA to understand how all the pieces fit together, we need to ask is that a program that is too big and too complicated to exist? Because if we can't be confident that the oversight is functioning, it's too dangerous to be there.

MR. WITTES: So we are going to go to questions. Please introduce yourself. Please state things in the form of a question. If you don't, I will use my prerogative and the Panopticon, all-seeing Panopticon that is here, to cut you off. And please direct all questions to one side or the other. And the format here will be side you

direct it to will get the first chance to answer and then the other side will get a chance to respond before we go to another question.

SPEAKER: I'm afraid I'm not going to meet your criteria.

MR. WITTES: Then woe betide you.

SPEAKER: Oh, okay. It just seems to me that the issue is not being addressed or the debate is not being addressed on an even scale. We have focused so much on collection and so little on the use of the data that is being collected and the benefit of that, and having a -- whether it's the Secretary of Defense or State or the President saying it's done real damage is not good enough. And I recognize the security problem of saying what is the benefit, but I wonder how the panel feels about the balance between collection, namely NSA which has been pinpointed, and all the users or analysts that are taking this data.

MR. INGLIS: That's a great question, so let me start from an NSA perspective. It turns out that when you read the governing regulations, largely what's been called Executive Order 12333 SIGINT is described as "special," right? That's why it was called "special intelligence." It used to be a big secret. When somebody would hand you a report and say this is from special intelligence, you knew immediately it was NSA.

Why is it special? Because there was a greater possibility that you would incur upon U.S. person communications. When you collected communications in the world there's always two sides to that communication. And because of that, in the dissemination phase there's a restriction that NSA can only disseminate largely finished product. Right? There has to be a minimization process that first occurs before you actually put that in the hands of someone else. And so there isn't unfettered access to this raw take that NSA might kind of bring in, within which we're looking for the national security issues and the reporting that we would then derive.

But nonetheless, the burden for handling this information the right way doesn't end at the moment of collection. Right? It actually continues all the way through the life of that information to include if we do package something into a report and give that to a customer -- Secretary of State, the President, somebody standing in harm's way -- there's a burden even at that point in time to protect that information appropriately, both from the standpoint of its classification and from the standpoint of the protection of any identities inside, whether they be national or kind of, you know, referred to as "U.S. persons." You have to actually have rules that say how do you protect that across the life of that product? And so you can't just say I'm done. I now have kind of Katy bar the door, unlicensed, unfettered access to this material simply because I got it.

MR. JAFFER: Well, the question of use is an important one. You know, I think that even if you accept that the government should be engaged in collection on this scale, you then have to address this question that you raise, well, what can the government then do with the information that it collects?

And one of the most, I think, troubling documents that's been released over the last year is the NSA's what they call minimization procedures relating to Section 702, which is the 2008 statute that Congress passed in order to expand the government's authority to collect one-end domestic communications, Americans' international communications. And the minimization procedures make clear that even though the government is targeting people outside the United States, this is a statute that allows them to target people outside the United States, the government is actually collecting large volumes of Americans' communications. And when those communications come in, they don't destroy Americans' communications. They don't even destroy quickly Americans' communications that have nothing to do with foreign intelligence. The minimization procedures allow them to keep those communications for up to five years

and to keep the indefinitely if the NSA concludes that the communications include what they call foreign intelligence information. And foreign intelligence information is defined very broadly to encompass even a conversation that relates to foreign affairs.

So, you know, even if you accept that there should be bulk collection on the front end, you have to ask this question whether the restrictions on the government's use of the information are stringent enough. And I think if you look at those minimization procedures, you'll see why a lot of people, including the ACLU, believe that they're not.

MR. WITTES: Ma'am?

MS. THOMPSON: Hi. My name is Sarah Thompson. Thank you so much for putting on this program. I think this is a very important discussion and debate.

I guess my main concern would be -- I have so many questions, but I'm going to go with my main concern -- is just from the interviews that I've listened to with Snowden and Glenn Greenberg [*sic*], it seemed as though there was one program in which the NSA was specifically rerouting Internet routers and specifically inputting a backdoor device on personal Internet routers, and so that they could collect as much information as possible from personal Internet routers that were ordered by American people. Now, as an American citizen that's very concerning to me because especially, as you mentioned, the Constitutional amendment to provide for the common defense was discussed, there is a Constitutional amendment to prevent the unreasonable search and seizure. And I think that that sort of program is very alarming.

And in addition to that, if the NSA is collecting this information, what are they doing to ensure that there aren't any other international communities that would be very interested in this information to protect the information for American citizens?

I don't think I articulated that very well, but.

MR. INGLIS: No, I think you did. I would say that, as you've articulated

it, the possibility that NSA would apply means and methods to go after servers owned by Americans to collect communications into or out of those, that would not only be inappropriate, it would be illegal. Right? Absolutely illegal.

Is that to say that NSA does or does not have capabilities to do similar things when the cause is right, when the necessity is appropriate? So let's say we're going after a rogue nation or some hostile power that actually is coming after coalition soldiers in a place like Iraq or Afghanistan, I hope we do have capabilities of that sort, but they must be applied in that context for that purpose. They cannot be applied to Americans in the way that you've described.

Can I just also offer that Mr. Snowden has said many things over the last year, possibly has been interpreted as saying many things. I'll just give you two as a case in point, right, that NSA has direct access, unfettered access to the servers of Google, Microsoft, you know, AOL. That's not true. That any analyst sitting at NSA could, at their discretion, target the communications of the President of the United States. That's, on the face of it, ridiculous, but would be grossly illegal; simply not true.

And so a description of capabilities that might be applied to those things that are appropriate and then extended to those things that are not appropriate is where, I think, we've gotten into a lot of difficulty over the last year.

MR. SANCHEZ: So it's, I think, better and worse than what you described, at least as has been reported. That is to say the report that has been published is (1) that these are routers that are bound overseas. These are things being shipped to other countries that are having backdoors or implants placed inside them, as reported. But the worst part is they're not personal routers. This isn't your Wi-Fi, isn't like your Apple Time Capsule that goes in your living room and, you know, you and your roommates share. It's network-level routers. It's the kind of router that controls the traffic

for a corporate-level network. And that I actually find more interesting because it suggests not simply an intent to spy on a particular person that might be of interest, but an attempt to preserve a capability to ensure that all networks here or abroad are accessible if there comes a need.

The documents have also suggested that there have been software problems with some of the implants, which, I think, just from a pure security perspective, sort of raised a red flag. You've got essentially firmware running on a very sensitive device, holding large amounts of people's communications that is not known to the manufacturer and, therefore, can't be sort of updated or modified by the manufacturer, or if it, you know, turns out to conflict with a new update, I think creates potential vulnerabilities in networks around the world. And so I think the effort to sort of ensure universal access in the event that you need to target someone in the future is a kind of mission intention with the security of global communications.

MR. DANZER: Thank you all for the thoughtful debate. This question is directed at Jameel and Julian. My name is Matt Danzer. I'm a law student at Columbia.

I'm wondering, you know, over the last year we've heard all the criticisms of the current NSA system and of the intelligence community at large, whether it be compliance, proportionality, necessity, constitutionality, et cetera. But there hasn't been much discussion about what reforms you would actually be comfortable with and what system you foresee as appropriate for both NSA and for the ACLU and other groups. And so what are your top however many reforms that would create a system that you see as proportionate, necessary, Constitutional, ensuring adequate compliance, not too secret but secret enough to get the job done?

MR. JAFFER: Well, we put out --

MR. WITTES: In 25 words or less.

MR. JAFFER: Yeah, sure. (Laughter) So we put out a very short briefing paper today that goes through some of the reforms that we think are necessary. But I'll tell you that in relation to the discussion we've had today, I think that the most important reform is foregoing bulk surveillance and replacing it with individualized surveillance. You can target people who you think are engaged in criminal activity, who are foreign agents. You can target the people whose communications you have a legitimate interest in monitoring, but you can't target everyone in order to get those communications. That's the basic principle.

I think that's the principle that the Fourth Amendment was meant to put in place. It was an answer to the general warrants and the writs of assistance that the Founders here found so objectionable. It's the same principle that we would put in place today. We think that that principle makes sense, that it accommodates the government's legitimate interest in tracking suspected terrorists, but it does it in a way that preserves civil liberties.

MR. SANCHEZ: I mean, the schematic answer is a return to particularity from a model of surveying populations or entire data streams in order to figure out what particular persons you're interested in, at least for more sensitive kinds of information that implicate, for example, First Amendment rights, like communications data. So, you know, we've already made one shift in that direction or at least declared our intention to shift in that direction from collect all the data, mine it in case it comes in handy in the future, to if you have a suspect, get an order, get their records and perhaps the records of people in direct contact with them. We're not doing it, I think, as tightly as the Senate did in 2005, when it unanimously approved language that was later removed in conference that would have required a sort of tighter nexus between the records you're obtaining and a particular suspected foreign agent. That kind of thing, I think, it makes sense.

On the 702 side, you know, we had a problem that was described with respect to communications that are fundamentally really international that sort of stop in the U.S. Someone sends an email, it sits on a server, and then it goes out again, but under the kind of old FISA definitions that looks like two one-end U.S. wire communications. And, you know, right, that's a problem, fine. But you need to adjust to the realities of the Internet and say, okay, a totally foreign communication that's stopping in the U.S. should perhaps not be treated the same way as a one-end U.S. communication.

We then changed the standard that would create these kind of blanket and general warrants that did not only apply to transiting communications, but also applied to communications traditionally regulated with one party inside the U.S. So a kind of balance that might be appropriate there is, you know, maybe permissively in cases where you can't tell, you can't always tell for certain, but in cases where you've got a foreign target, targeted because they're foreign -- they don't have to be shown to be terrorists or spies or anything -- and there is reasonable evidence suggesting that the communication's not just passing through, but is with a U.S. person, in that condition you get a warrant. I don't think it was a good reason to remove those from the authority of the FISA Court, as we ended up doing in 2008, in order to solve this other problem.

MR. WITTES: Go ahead.

MS. CORDERO: So a few thoughts. First, I think Julian just made a comment that someone shouldn't be targeted just because they're foreign. NSA is in the foreign intelligence collection business, so they're not targeting people just because they're foreign. They're targeting people to collect foreign intelligence information as it's been defined in an Executive Order for over 35 years. So that definition hasn't changed. It's nothing new. It didn't just come out in the last year since the Snowden revelations.

That's how the NSA has done its business for some time.

On the proposals to outlaw bulk collection, I really think that they're shortsighted because what they're in effect saying is that the entire world communicates digitally, information now resides in pots of data and we are okay with the whole world communicating that way except we want our national security folks to do their business on onesies and twosies and basically go back to file-and-paper system, and that is just not realistic. And so I think that where we're going to end up is in a situation where information that is needed for foreign intelligence purposes, national security protective purposes, is retained in a certain way. We will have outlawed by statute. And some executive down the road is going to be in a difficult place.

MR. WITTES: Okay, so we have about two minutes left and so what I'm going to do is ask -- we have three people who have been waiting very patiently: the gentleman there, the gentleman there, and Shane Harris. So let's just --

SPEAKER: Also a gentleman.

MR. WITTES: Also a gentleman over there. So we're going to take those three questions and then give each side a chance to wrap up. Sir?

MR. PIERCE: So my name is Todd Pierce. I'm a retired Army officer.

Putting aside that last straw man argument and also putting aside Geoffrey Stone as being authoritative, I would say that he is infallible -- rather, he's not infallible having read him, but, anyway, the Vietnam War was the most costly war in lives and money to the United States, the most detrimental to our large-term strategic interests, I think, everybody would agree who are familiar with it, since World War II. But yet during that time we had dissenters saying we've got to get out, this is a wasteful war, we're being harmed by it. General Weyand said it was unwinnable from the very beginning. Yet, the Department of Defense and through the Army were spying on

American citizens to suppress dissent against the war, which later turned out, as we can now know with hindsight, was the most beneficial we had, was to get out of it, contrary to people like General Westmoreland, who was lying and manipulating intelligence.

So tell me what guarantees there are with all the data that's being collected in the gigantic storage system being built on Salt Lake City to be available with just a keystroke to any government official, like the Department of Homeland Security or the FBI? What guarantee can you give us that our civil liberties, which are really intended to provide for our strength because we have that right to dissent unlike Communists and other authoritarian countries, what guarantee can you give us that we're not going to be able to -- your agencies that you represent and the ones they give information to will not suppress dissent when we get into some harmful situation like that again perhaps and we need that dissent to get us out of the harmful situation?

MR. INGLIS: Yes, only first degree that --

MR. WITTES: Let's take the other questions first. Sir?

SPEAKER: I'm Raphael from Brazil. My question goes to Carrie and Chris.

The United States says it doesn't engage in economic espionage, so I would like you to explain why the NSA spied on Petrobras, the Brazilian oil giant. And what was the national security threat behind that oil company? Thank you.

MR. WITTES: Shane?

MR. HARRIS: Okay. And for Jameel, given that you work for an organization that is in touch with people whom the NSA might consider legitimate targets for foreign intelligence purposes, including, I would argue, Edward Snowden, do you think that you are or have ever been subject to FISA surveillance? And to Carrie, do you think he should be? (Laughter)

MS. CORDERO: Of course not.

MR. WITTES: Okay. We're going to give -- let's give the pro side an opportunity to wrap up first.

MS. CORDERO: I'm going to say no to Shane right off the bat.

(Laughter)

MR. HARRIS: I'll answer that after the event.

MR. SANCHEZ: I imagine not a subject, although, you know, it wouldn't shock me if I had been something sucked up in the process of talking to someone else outside the country. Actually I might want to refine that slightly. You talk about the guarantee we have that something won't be turned to the kind of use you're concerned about and, I mean, actually it occurs to me that it's not a bad test, which is to say not -- there are all the rules and procedures in place now, which, of course, there are, that would not permit what you're talking about. But I think a decent test is take in the aggregate the architecture that has been constructed involving often equipment implanted directly on the Internet backbone and in some of these companies, and ask not what could legally be done now, but in the aftermath of an attack, let's say by some fringe part of Occupy or the Tea Party, if you have a President delivering an Executive Order saying go after those folks, how long would it take to change the architecture, to turn that architecture to an illegitimate purpose? And if the answer is it would take a couple lines of code and a switch being flipped, that's a dangerous architecture. If it's not an architecture that would respond that quickly, it's less dangerous architecture.

MR. WITTES: Guys?

MR. INGLIS: Yeah, so if I could just respond to the questions briefly.

So first to the gentleman, thank you for your service in the United States Army. We all appreciate that. I would say that the kind of transgressions that you

describe from the 1960s were real. They were proven. They were the subject of the Church-Pike Commissions. We have taken the lessons from that as a national security apparatus and as a government. Right? There was essentially a complicity across the government in that, and have affected the way that we allocate these authorities, the way that we govern the execution of these authorities, and the way we account for the implementation of those authorities -- three phases -- across multiple branches of government. That's, I think, the same kind of thing that Madison, as we referred to earlier, would have intended in this government, that there are checks and balances.

You know, people are naturally suspicious of this government because it's inbred. Right? It's essentially written into the Constitution. We must always be naturally suspicious of this government, but we shouldn't be cynical. We should, in fact, understand that people who take the oath attempt to try to get that right -- balance, the privacy, the national security -- and affect sufficient transparency -- oversight and accountability -- to pull that off.

To the point of economic espionage, we don't do economic espionage, and I'll just leave it at that, period.

And with respect to constituting a FISA surveillance of Jameel and Julian, I'm shocked, right, that that would be possible. (Laughter)

MR. WITTES: That's going to have to be the last word. Jameel gets away without FISA surveillance. Please join me in thanking our panel for a great debate. (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

)Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016