



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction

Location: Newseum Knight TV Studio, Washington, D.C.

Date: Tuesday, June 25, 2013 Time: 4:00 p.m. EDT

Welcome by: James Duff, President, Newseum Introduction by: Laurel Bellows, President, American Bar Association

Moderator: Harvey Rishikof, Chair, American Bar Association Standing Committee on Law and National Security of the Advisory Committee

Panelists:

- Robert Litt, General Counsel, Office of the Director of National Intelligence;
- M.E (Spike) Bowman, Professorial Lecturer, The George Washington University; Former Deputy National Counterintelligence Executive;
- Kate Martin, Director, Center for National Security Studies;
- Gene Policinski, Executive Director, First Amendment Center;
- Ellen Shearer, William F. Thomas Professor of Journalism and Co-Director, Medill School of Journalism, Northwestern University;
- Joel Brenner, Former Inspector General, National Security Agency; Former National Counterintelligence Executive
- Stewart Baker, Partner, Steptoe & Johnson; Former General Counsel, National Security Agency

JAMES DUFF: Good afternoon, everyone. I'm Jim Duff. I'm president here at the Newseum. And this is a very special day for us at the Newseum as we launch our Newseum Institute, officially tomorrow, but the first – very first program of our institute, which will be really devoted to civil education of the public about very important First Amendment issues, will be a collaboration of all of our educational outreach programs.

We are just delighted that today is the day that we're going to launch it here at the Newseum. And what better way and what better topic – nothing could be more topical or informative and



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

important to us all as Americans as the current events involving NSA surveillance leaks. And it's our particular pleasure to co-host this event today with the American Bar Association – we're delighted that they have really put together a wonderful lineup of panelists who will be introduced to you shortly – the Medill School at Northwestern University and the McCormick Foundation are all co-hosts along with us here at the Newseum of this important discussion.

And before introducing you to the president of the American Bar Association, I do want to say a special thank you to my dear friend, Harvey Rishikof, who will be moderating the program this afternoon. Harvey was my predecessor in Chief Justice Rehnquist's chambers, in a position now called counselor to the chief justice. When Harvey and I held that position, it was called administrative assistant the chief justice. So they waited till we got out of there and then upgraded it to counselor, which sounds much more important and – the same job though, nonetheless. Harvey was very, very helpful to me in transition in the chief justice's chambers.

I think you will agree with – based on the turnout here this afternoon for this program, I think you'll agree with me as to how important this topic is to all of us as Americans. And we want to get right to it. So I do want to now introduce you to the president of the American Bar Association, Laurel Bellows, who has quite a distinguished career and heads the Bellows Law Group in Chicago and is a great leader of the American Bar Association.

Laurel, welcome. (Applause).

LAUREL BELLOWS: Thanks, Jim. And thanks for your introduction. And there's no way of thanking you enough for being a co-host of this event with the – with the Freedom Center and the First Amendment Center and Medill School of Journalism at Northwestern University. I'm a Chicagoan, so I get to shout-out for Northwestern, not simply the Blackhawks, but Northwestern, right? (Laughter).

And a special thanks to Robert R. McCormick Foundation for its help in presenting this program here today and for the ABA Standing Committee on Law and National Security, which is the oldest committee at the American Bar Association and, of course, the organizer of this event. And before I say a few words about why we're here and what we're doing, again, a shout-out from me to Harvey Rishikof, who – without his opening his rolodex today and understanding the crucial nature of beginning this conversation, we would not be here today with the stellar panel that you are about to meet.

We are all aware that, as time goes by, our lives are under increasing surveillance. Nevertheless, the existence of PRISM and the vastness of its scope came as a surprise to Main Street America. Many have framed the PRISM controversy in terms of how much surveillance is



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

acceptable. And anything in excess of acceptable is, a priori, an infringement of our Constitutional liberties.

As lawyers, we should not be willing to accept sound bite Constitutional analysis. We should also not be too quick to applaud our ability as a society to obtain pictures of the Boston Marathon bombing suspects within hours or even minutes but at the same time condemn more sophisticated surveillance. I, for one, am not persuaded that the analysis of what kind of surveillance is legally improper depends on the method used to obtain the information or even the number of gigabytes obtained.

We are a nation of laws. Consequently, we should be concerned with whether checks and balances are in place, who authorized the surveillance, under what authority, has that authorization been reviewed to determine whether it was lawful? American lawyers have the obligation to be heard on matters affecting what we do to protect our rights and liberties in the context of assuring the security of our society and our nation.

The views you will hear today don't necessarily represent the views of the American Bar Association as a whole. Our membership, like all of you, is involved in a learning process. It's my hope that other ABA sections and voices will be heard, and in the coming weeks we'll present other perspectives so that most importantly, we can have in this country a full and informed debate.

And now it is my pleasure to turn this program over to its organizer, Harvey Rishikof, who will serve as our moderator. Thank you. (Applause).

HARVEY RISHIKOF: OK. Good afternoon. Thank you for coming.

I have a few housekeeping rules that I have to get out of the way. The first is that we are using this a – the Newseum, and we are going to be using all the modes of communication.

So we have a Twitter account. And that's hashmark A-B-A-N-A-T-S-E-C, #abanatsec. And I encourage everyone to tweet us. And we'll have someone looking at the tweets, and they'll be able to pass the questions up to the podium. We also have an email way of getting questions to us for the audience who's not here. And that's ahampton, A-H-A-M-P-T-O-N@freedomforum.org. Again, it's ahampton@freedomforum.org.

And then the people who are in the audience, we've handed out on your seats some small notecards. And we'll be collecting the notecards every 30 minutes or so. Just pass them out to the end, and we have people who are going to be collecting them. And we'll have someone



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

look at those and pass those cards up to me for when we have to do questions.

So let me begin by saying that I want to thank so much Jim at the Newseum – as he said, I'd like to think I lowered the bar, and Jim raised it, when I was working at the Supreme Court – and Laurel, for all her support and what she has done to make this issue of cyber and cyberrelated privacy a forefront of her stewardship at the ABA presidency. And I have to thank our sponsors, which also is the Medill group from Northwestern and the McCormick Foundation, who also have been with us and able to put this forward.

Our committee is, as Laurel noted, is 50 years old, and it's a committee that really has always tried to focus on these hard issues and bring the issues to the public and have an open and fair discussion as to what the reality is and what the fiction is. That's why we entitled this particular program, as you see, facts and myth.

As you know, what kicked off this issue was the NSA PRISM program, which emerged as a result of a disclosure made by Edward Snowden, an NSA contractor employee. The first random disclosures have touched the hot-button topics of government secrecy, intrusion into American citizens' privacy interests and the beginning of the year of big data. National security and protecting privacy are becoming the central interest of the emerging technological revolution. And the question we have is how democracies and emerging democracies create frameworks for these vital interests.

Another aspect of this particular issue – it's why we have panelists, and I'll be introducing them shortly – is the issue of this topic touches the First Amendment. It has clear implications regarding the news media. Who and what is a journalist in the 21st century? How do journalists deal with circumstances such as the PRISM disclosure and the Wikileaks massive document, quote, dump, close quote, that circumvented traditional news organizations? Where can the public find accurate information on both disclosures and government response?

That is why we're having this panel. And if you – for the audience, they have the – they have the backgrounds of the panelists. But I think we've assembled one of the more extraordinary groups of expertise that we can. I'll just do it – it looks like alphabetical order, which is:

Stu Baker, who's the former general counsel of the National Security Agency and has had quite a career, both with DHS, where he was set up at the policy shop, and has been – has a – is with Steptoe currently and has had quite a practice and involved in these issues and has been appearing quite regularly in most places that one wants to look at for this type of information and also has a book out called "Skating on Stilts: Why Aren't We Stopping Tomorrow's Terrorism."



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

Beside him is Joel Brenner. Joel comes to us – is now in his own private practice. He also is a(n) author. His book is entitled “America the Vulnerable: Inside the New Threat Matrix of Digital Espionage Crime and Warfare.” He has an extensive background in these areas. He was a senior counsel at the National Security Agency; he was also, until – from 2006 to 2009, he was the head of U.S. counterintelligence at the DNI. He also served at the prosecutor in the Justice Department’s Antitrust Division and has extensive trial and arbitration experience in a variety of these areas.

Sitting beside him, if I can see, is Kate Martin. Kate joined, as you know from the program, is the director of the Center for National Security Studies. She joined the center in '88; she is the director of its litigation project. She has served in the center since '82, she teaches national security law as a professional lecturer at GW, and she also teaches at Georgetown University. She has served as the general counsel of the nation’s National Security Archive and as a research librarian located in GW from '95 to 2001. She is also a member of the Liberty and Security Initiative of the Constitutional Project. She testifies quite regularly on the Hill on these and related issues.

Beside her is Gene Policinski, who is chief operating officer of the Newseum and has just – I think as was announced – has become the president of the First Amendment Center, one of the institution’s programs. He’s a veteran journalist, has held news leadership positions in newspapers and radio and television. He co-writes the weekly nationally distributed column, “Inside the First Amendment,” and attended National School of Law and has been really instrumental in putting this particular program together. And it’s our hope, if it goes well, that the AVA and Newseum will do more things together.

On his right is Ellen Shearer. Ellen has worked with us before in a number of programs, including a book that we worked on together with the AVA, which is entitled “National Security Laws in the News,” and I’ll be quoting from it periodically. It has some excellent chapters on – if someone was a journalist and wants to understand what the issues are in national security.

She is also a professor and is teaching – I think her full title is the William F. Thomas professor at the Medill School of Journalism, Northwestern. She’s co-director of the school’s national security journalism initiative; she was director of the Medill Washington Program until 2012. Before joining the faculty, she has over 20 years of experience in news industry and was a senior editor at NewsDay, and also at Newhouse News Services. She is the co-author of a number of books, including “Novoters: America’s No-Shows.”

Beside her is Spike Bowman. I have known Spike for many, many years as he’s a legendary



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

figure in the intelligence community. He's now a professional lecturer at GW, he specializes in national security law and policy. He was most recently the deputy at the National Counterintelligence Executive. He served as a senior research fellow at NDU, the National Defense University. And – but he served in the senior executive service at the Federal Bureau of Investigation as senior counsel; it's when I spent the most time with him. And he's been involved in these issues for many, many years, and he's actually a retired Navy captain and has authored a number of books and articles on these issues.

And I save – last is Bob Litt. I particularly want to thank Bob for coming. Bob is also someone who I was – had the honor to serve with in government, and Bob is the general counsel of the Office of Director of National Intelligence. Before joining ODNI, Bob was a partner with the law firm of Arnold and Porter. He served as a member of our advisory committee to the Standing Committee on Law and National Security and he also served as deputy assistant attorney general in the criminal division and was what we called the PADAG, the principal associate deputy attorney general, for the Department of Justice. We think PADAG is one of the best jobs you can have at DOJ; you sit between the attorney general and the deputy attorney general and you're in the hot seat.

And what I particularly want to thank Bob for doing is coming here today in order to represent this – the government's position in a sense of making it clear, what are facts about the program and what has been fantasy about the program.

And what we're going to do for the order of the – of the program is we'll let Bob lead off and then we'll fold in the other panel members, who will be able to respond, ask questions and may take positions on this issue. And interspersed, we'll be asking questions, either from the audience that's here or from the digital audience that exists out there that will be having questions sent to us.

So with that is the opening. Bob, I've – can you give us a sense of what the fact and fiction is on these programs that are known as PRISM, and inside the Beltway, we know them as 702 and these other notions of the Patriot Act? What's your – can you give us a sense and set the table for us to begin the discussion?

ROBERT LITT: Sure. Thanks, Harvey. There seem to be too many individuals and organizations to thank individually here, so I'll just endorse what Harvey said about the opportunity to come here and actually talk about this program.

I'm reminded a little bit of a quote that, like many quotes, is attributed to Mark Twain but in fact is not Mark Twain's, which is that a lie can get halfway around the world before the truth gets its



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

boots on. And unfortunately, there's been a lot of misinformation that's come out about these programs. And what I would like to do in the next couple of minutes is actually go through and explain what the programs are and what they aren't.

I particularly want to emphasize that I hope you come away from this with the understanding that neither of the programs that have been leaked to the press recently are indiscriminate sweeping up of information without regard to privacy or constitutional rights or any kind of controls. In fact, from my boss, the director of national intelligence, on down through the entire intelligence community, we are in fact sensitive to privacy and constitutional rights. After all, we are citizens of the United States. These are our rights too.

These programs, in fact, represent a careful effort to achieve the goals both of national security and of protection of individual rights. And they do this by a combination of restrictions on what kind of information can be collected, restrictions on how that information can be kept and used and multilayered oversight procedures.

So as I said, we're talking about two types of intelligence collection program. I want to start discussing them by making the point that in order to target the emails or the phone calls or the communications of a United States citizen or a lawful permanent resident of the United States, wherever that person is located, or of any person within the United States, we need to go to court, and we need to get an individual order based on probable cause, the equivalent of an electronic surveillance warrant.

That does not mean and nobody has ever said that that means we never acquire the contents of an email or telephone call to which a United States person is a party. Whenever you're doing any collection of information, you're going to – you can't avoid some incidental acquisition of information about nontargeted persons. Think of a wiretap in a criminal case. You're wiretapping somebody, and you intercept conversations that are innocent as well as conversations that are inculpatory. If we seize somebody's computer, there's going to be information about innocent people on that. This is just a necessary incident.

What we do is we impose controls on the use of that information. But what we cannot do – and I'm repeating this – is go out and target the communications of Americans for collection without an individual court order.

So the first of the programs that I want to talk about that was leaked to the press is what's been called Section 215, or business record collection. It's called Section 215 because that was the section of the Patriot Act that put the current version of that statute into place. And under that – this statute, we collect telephone metadata, using a court order which is authorized by the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

Foreign Intelligence Surveillance Act, under a provision which allows a government to obtain business records for intelligence and counterterrorism purposes. Now, by metadata, in this context, I mean data that describes the phone calls, such as the telephone number making the call, the telephone number dialed, the data and time the call was made and the length of the call. These are business records of the telephone companies in question, which is why they can be collected under this provision.

Despite what you may have read about this program, we do not collect the content of any communications under this program. We do not collect the identity of any participant to any communication under this program. And while there seems to have been some confusion about this as recently as today, I want to make perfectly clear we do not collect cellphone location information under this program, either GPS information or cell site tower information. I'm not sure why it's been so hard to get people to understand that because it's been said repeatedly.

When the court approves collection under this statute, it issues two orders. One order, which is the one that was leaked, is an order to providers directing them to turn the relevant information over to the government. The other order, which was not leaked, is the order that spells out the limitations on what we can do with the information after it's been collected, who has access, what purposes they can access it for and how long it can be retained.

Some people have expressed concern, which is quite a valid concern in the abstract, that if you collect large quantities of metadata about telephone calls, you could subject it to sophisticated analysis, and using those kind of analytical tools, you can derive a lot of information about people that would otherwise not be discoverable.

The fact is, we are specifically not allowed to do that kind of analysis of this data, and we don't do it. The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts. All that we get under this program, all that we collect, is metadata. So all that we get back from one of these queries is metadata.

Each determination of a reasonable suspicion under this program must be documented and approved, and only a small portion of the data that is collected is ever actually reviewed, because the vast majority of that data is never going to be responsive to one of these terrorism-related queries.

In 2012 fewer than 300 identifiers were approved for searching this data. Nevertheless, we collect all the data because if you want to find a needle in the haystack, you need to have the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

haystack, especially in the case of a terrorism-related emergency, which is – and remember that this database is only used for terrorism-related purposes.

And if we want to pursue any further investigation as a result of a number that pops up as a result of one of these queries, we have to do, pursuant to other authorities and in particular if we want to conduct electronic surveillance of any number within the United States, as I said before, we have to go to court, we have to get an individual order based on probable cause.

That's one of the two programs.

The other program is very different. This is a program that's sometimes referred to as PRISM, which is a misnomer. PRISM is actually the name of a database. The program is collection under Section 702 of the Foreign Intelligence Surveillance Act, which is a public statute that is widely known to everybody. There's really no secret about this kind of collection.

This permits the government to target a non-U.S. person, somebody who's not a citizen or a permanent resident alien, located outside of the United States, for foreign intelligence purposes without obtaining a specific warrant for each target, under the programmatic supervision of the FISA Court.

And it's important here to step back and note that historically and at the time FISA was originally passed in 1978, this particular kind of collection, targeting non-U.S. persons outside of the United States for foreign intelligence purposes, was not intended to be covered by FISA as – at all. It was totally outside of the supervision of the FISA Court and totally within the prerogative of the executive branch. So in that respect, Section 702 is properly viewed as an expansion of FISA Court authority, rather than a contraction of that authority.

So Section 702, as I – as I said, it's – is limited to targeting foreigners outside the United States to acquire foreign intelligence information. And there is a specific provision in this statute that prohibits us from making an end run about this, about – on this requirement, because we are expressly prohibited from targeting somebody outside of the United States in order to obtain some information about somebody inside the United States. That is to say, if we know that somebody outside of the United States is communicating with Spike Bowman, and we really want to get Spike Bowman's communications, we've got to get an electronic surveillance order on Spike Bowman. We cannot target the out – the person outside of the United States to collect on Spike.

In order to use Section 702, the government has to obtain approval from the FISA Court for the plan it intends to use to conduct the collection. This plan includes, first of all, identification of the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

foreign intelligence purposes of the collection; second, the plan and the procedures for ensuring that the individuals targeted for collection are in fact non-U.S. persons who are located outside of the United States. These are referred to as targeting procedures. And in addition, we have to get approval of the government's procedures for what it will do with information about a U.S. person or someone inside the United States if we get that information through this collection. These procedures, which are called minimization procedures, determine what we can keep and what we can disseminate to other government agencies and impose limitations on that. And in particular, dissemination of information about U.S. persons is expressly prohibited unless that information is necessary to understand foreign intelligence or to assess its importance or is evidence of a crime or indicates a – an imminent threat of death or serious bodily harm.

And again, these procedures, the targeting and minimization procedures, have to be approved by the FISA court as consistent with the statute and consistent with the Fourth Amendment. And that's what the Section 702 collection is.

The last thing I want to talk about a little bit is the myth that this is sort of unchecked authority, because we have extensive oversight and control over the collection, which involves all three branches of government. First, NSA has extensive technological processes, including segregated databases, limited access and audit trails, and they have extensive internal oversight, including their own compliance officer, who oversees compliance with the rules.

Second, the Department of Justice and my office, the Office of the Director of National Intelligence, are specifically charged with overseeing NSA's activities to make sure that there are no compliance problems. And we report to the Congress twice a year on the use of these collection authorities and compliance problems. And if we find a problem, we correct it. Inspectors general, independent inspectors general, who, as you all know, also have an independent reporting responsibility to Congress, also are charged with undertaking a review of how these surveillance programs are carried out.

Any time that information is collected in violation of the rules, it's reported immediately to the FISA court and is also reported to the relevant congressional oversight committees. It doesn't matter how small the – or technical the violation is. And information that's collected in violation of the rules has to be purged, with very limited exceptions.

Both the FISA court and the congressional oversight committees, which are Intelligence and Judiciary, take a very active role in overseeing this program and ensuring that we adhere to the requirements of the statutes and the court orders. And let me just stop and say that the suggestion that the FISA court is a rubber stamp is a complete canard, as anybody who's ever had the privilege of appearing before Judge Bates or Judge Walton can attest.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

Now, this is a complex system, and like any complex system, it's not error free. But as I said before, every time we have found a mistake, we've fixed it. And the mistakes are self-reported. We find them ourselves in the exercise of our oversight. No one has ever found that there has ever been – and by no one, I mean the people at NSA, the people at the Department of Justice, the people at the Office of the Director of National Intelligence, the inspectors general, the FISA court and the congressional oversight committees, all of whom have visibility into this – nobody has ever found that there has ever been any intentional effort to violate the law or any intentional misuse of these tools.

So that's a brief overview of the program. I'll be glad, after the others speak – I suspect that there may be one or two questions to directed at me, and that's what I'm here to answer.

MR. RISHIKOF: Thank you, Bob. Excellent job of laying the issue out as to what the facts are from the perspective of the government.

So Kate, you've been active in this area for many, many years. What has Bob said that you think does not rise to either statutory or constitutional protection?

KATE MARTIN: Well, I've known Bob for many years, and I'm sure everything he said was correct, but I do disagree about the significance of the authorities and the programs that he laid out. And I want to start maybe by making the provocative comment that, you know, the American people shouldn't be treated as idiots. If what Bob has just laid out had been told to the American public at the time when Congress was debating what the scope of surveillance powers should be, it might well be that we would have less public distrust of the government, and maybe even Snowden wouldn't have done what he did and made such a big splash.

I think there are two separate issues raised by the revelations. The first set of issues goes to the question of First Amendment protections and the requirement that I think is a constitutional one, that the public has a right to know what its government's doing and that we don't operate under a system of secret law. The second set of issues are about the privacy rights of Americans.

And I'll just make a couple of comments about the first. I think that the basic issue raised by the disclosure on the First Amendment side of the 215 program – which is a program that Bob described as collecting all of the telephone metadata of all domestic phone calls in this country – is that we didn't know that the law had given the government the authority to do that. I've been involved in these debates for longer than I would really care to think about, and we were worried about that. And in 2006, when the secret NSA spying programs were first revealed by



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

The New York Times and then by follow-up news stories, what happened after that is that in the next two years, Congress sat down and said, do we need to change the law in order to authorize some of this, in order to prevent some of this? What do we need to do? And in that debate, the government was conspicuously silent about the fact that it had decided that Section 215 would allow it to collect – to do this bulk collection program of telephone metadata.

Since then, members of Congress, civil liberties community have been asking over and over again about how the FISA court and the government interprets its authority and no answer has been forthcoming. I guess since I'm lucky enough to be on the stage with Bob, I would pose a couple of other questions that we don't know about secret law at the moment, which is whether or not the same 215 authority which is being exercised to get telephone metadata in bulk could be used to get credit card records in bulk or bank records in bulk, because when you read the text of the statute there's – it treats all those records the same.

On the privacy questions, so I think there's a couple of important points. One is this distinction between content and metadata or content and noncontent. And it is definitely true that the Supreme Court has said that the Fourth Amendment protects content more – in a way – and it does not protect noncontent or metadata.

One of the issues that's been debated and is, I think, a crucial issue for us to face as a country, is whether or not that Supreme Court analysis, which was made in 1976, is outdated and whether or not its understanding of the limits of the Fourth Amendment doesn't make sense in a society where metadata, noncontent information, when collected by the government and analyzed by computers, may be more revealing of an individual's personal activities and associations than listening to their telephone conversations or reading their email.

Now one of the answers to this is, well, the programs that were leaked are very specific and narrower programs. But one of the things that I think we need to know and we need to discuss in this country is what is the overall scope of the government's collection authority on personal information about Americans, because these are two specific provisions of statutes that go on for many pages, on telephone metadata. As far as I can determine, there are at least four, if not more, separate statutes that would allow the government to collect telephone metadata. They have different standards, they require different things, and one of the problems that we've had is the government says, well, we're not collecting over here. But guess what? We're not going to tell you we're going to collect over here. And we have an incomplete picture of what the government's overall legal powers and authorities are to collect very sensitive information about Americans. So maybe the final point that I'll make is we've always agreed that there are legitimate government secrets and that a democracy, like any other country, can't operate without keeping legitimate secrets secret. I think this – these events raise two important questions.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

One is are we going to understand that if the government is collecting intelligence on Americans, that because as a general matter, we've always understood that intelligence activities are probably secret, we're going to bootstrap – I'm sure my colleagues would disagree, but – and say that the law – the scope of the law and the scope of the power that the government has also has to be secret? That's an enormous leap, which I think needs to be debated. And I guess the other question I think that's raised is whether or not, from the standpoint of doing a good job, has the government really looked at the problem of keeping secret what really needs to be secret in this day and age, given the electronic snooping that's available, given the massive amount of information that's out there and given the massive number of people who now have security clearances and apparently enough high-tech skills to break all rules? And that's – OK.

MR. RISHIKOF: Great. I think you've set – both of you have really set the table.

Stewart, you were at the NSA during a large number of these periods. Can you give a sense of – your sense of whether or not there was a surprise in interpretation of 215 and what your sense is when you were at Homeland Security, what you needed in order to be able to –

STEWART BAKER: Yeah, I was – I will say I was a little surprised, although that was partly because many of the limitations were not disclosed by the people who called themselves reporters. They had these minimization documents. They had these targeting documents, which, as we've heard, are central to understanding what was going on and to realizing that many of the misimpressions that you could have pulled from the bare order or those incorrect slides were only part of the story.

They had it for two weeks and never disclosed it. I don't understand how a reporter justifies withholding information that's central to the context of the story for two weeks unless, you know, frankly, you're Andrew Breitbart. Andrew Breitbart, as an advocate – Andrew Breitbart was a great newsmaker, and he did a lot of hidden videos of bureaucrats saying things they shouldn't say. And he withheld some of the videos so that when the bureaucrats and the unions that he was targeting defended themselves, they said things that he knew they were going to say that weren't true, and he could prove it by releasing more stuff.

Now, that's a great advocacy tactic. If you're a newsmaker, that's great. But if you're the reporter, is that how you treat your – do you treat the American people like idiots, to coin a phrase, that can be manipulated and kind of stampeded into a view of the law that you know is not correct, when you save the documents until you can use them to contradict something that the government has said?



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

I called out Glenn Greenwald on this and Bart Gellman on that, and they responded quite in character. Gellman said quite truculently, yo, the Post did the same thing; do they hate America too? And Bart wrote a thousand words. A – but – and I've put it on my blog, skating on Stilts, if you want to read it. But it – I don't think either of them fully defended themselves from the accusation of what they did. Their withholding of that information was the act of an advocate who had an ax to grind and wanted to create an impression that disclosing these documents earlier would not have allowed them to create.

MR. RISHIKOF: Joel – and then we'll get to the journalist issue that you raised. But Joel, you were an IG, inspector general. You were involved in policing many of these programs. What is your sense about the interpretation and how you went about doing your job?

JOEL BRENNER: I think there's some force in the notion that – well, let me begin this way, Harvey. You know, democracies distrust powerful secret organizations. Our intelligence agencies are powerful and secret, for the reasons Kate explained. How do we square that circle? How do we make the exercise of these secret functions acceptable in a democracy?

And the only way we do it is if the rules under which they operate are, generally speaking, public, certainly at a strategic level and if we have mechanisms in place to give us a high degree of assurance that the rules are being followed.

Now, I don't believe in secret laws. And I think there is, as Stewart indicated, I agree, there's considerable room here to believe that even pretty close observers didn't know exactly what – some of the metadata that was being collected. I think that, you know, in general the intelligence community wants to hold those things close to the vest because they feel that the disclosures will cost them a certain amount of tactical advantage. This is true. But there's a strategic advantage in having the country unified behind the activities that are in question.

And I would like to see more disclosure and less classification. I think we have a significant overclassification problem. But I would like to come back, Harvey, to the big picture, and take off from something – the beginning and end of what you said, Kate. You began by saying that we don't want secret law. The public has the right to know certain things, although there's not a general right to know everything. It's good to remember that. And you ended by saying that there are certain things we have to have that have to be secret.

Explaining and figuring out where that line is, is not a task that's over and done with. It's continuing and it's difficult. Americans ought to know that we're the first country, I think on Earth, and certainly the first major power, to turn intelligence into a regulated business. None of



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

our European friends have anything like the oversight mechanisms that we have in our republic looking over our intelligence functions.

As Bob said – began by saying, we have all three branches of government involved in this. This is not a case contrary to what one sometimes hears of the intelligence community saying, oh, trust us; we'll follow the rules. I, for one, would not support an – such a regime. We have powerful intelligence communities that really do pull a leash on the Hill that we've had since 1976 and 1977. We have a special court composed of federal judges who rotate through these functions, who actually have a window into what's actually happening.

It's one thing to pass stringent rules about the intelligence activities. Lots of countries do that. But we actually police them with heavily staffed organizations that have no parallel in any European parliament, let alone in countries like Russia or China. We actually do this. And I know because I started that auditing process at NSA when I was the inspector general. We look at what's actually being collected. And the FISA Court looks at this stuff.

And as Bob said, with all this metadata that's being collected, they only looked at 300 cases last year. That's a drop in the bucket. What they've really do is to separate search from seizure. They've taken this stuff, but they have the most stringent rules that govern when it can be looked at. Now, why do they need it? You might say – good question.

Why do they need the older data? Why don't they just wait till they find somebody overseas who's talking to somebody in the United States and find out then who that person's talking to? Because they want to find out who he was talking to yesterday and last month for the very good reason that we don't want any more Bostons.

MR. RISHIKOF: Thank you, Joel. Thank you. So I'm going to give you a quick response, Bob. And one of the – then we'll turn to the journalist sort of aspect that has been raised by the other participants.

But one question we've had, Bob, is there is a Privacy and Civil Liberties Oversight Board which is also supposed to be part of this structure in the government. And they've been a bit quiet, I think, for a while. And sort of the interesting question is how you see them fitting into the – sort of this structure, and then responding to what – the points that have been put on the table so far.

MR. LITT: So in terms of the Privacy and Civil Liberties Oversight Board, they are very actively involved in this. They've gotten briefed on these programs. I think they are planning on holding a public event to discuss the surveillance programs in early July. And I think that the – that the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

president met with them the other day. So I think they're going to be very – their job is precisely to look at this intersection of national security and privacy and civil liberties, and I think they're going to be very actively involved in that, and we welcome that as another oversight thing.

The only point I want to respond to is I think Joel had it exactly right that everybody – or at least everybody responsible – agrees that on the one hand, there are some things that need to be secret and on the other hand we should disclose as much as we possibly can. And the disagreement is over – is in part over where that line is drawn.

But I firmly believe the disagreement is also over who draws that line. And I'm pretty much of a hard-liner on this. I do not think that the line for appropriate disclosures should be drawn by individual people who may have more agenda than information and who make a determination that the decisions that are made by the executive, legislative and judicial branches about what – where the line needs to be drawn to protect national security, that in one individual's view, those are wrong.

I – I'm not an alarmist. I'm – I don't – I'm not a longtime intelligence professional. I've only been in this job for four years. I came from this – to this position from the criminal law. But I can tell you that these disclosures are going to have consequences. It's going to take some time to determine how much the consequences are going to be, but we are going to lose collection capabilities, not only against terrorists but other foreign intelligence collection capabilities. That's a cost.

We collectively as a nation made a decision some years ago that the proper way to balance public oversight and the need for intelligence secrecy is through the intelligence committees of the Congress. The intelligence committees have been absolutely fully informed about both of these programs, as indeed they're informed of all collection activities. And indeed before the Congress voted in – within the last couple of years, both of these statutes have been reauthorized, and before they were – before they were passed by Congress, information about these programs was made available to every single member of Congress. That's the way that we've chosen as a nation to conduct oversight. If we want to conduct oversight about intelligence in the open, that's great for transparency, but we won't have much of an intelligence collection apparatus if we do that.

MR. RISHIKOF: So – thank you. So the Congress is involved, the executive branch is involved, the judiciary's involved. But clearly what really kicked the story was the fourth estate. So, Ellen, what is your sense, sitting there, hearing this debate about the role and function of the fourth estate in this particular issue?



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

ELLEN SHEARER: Well, I think that the reporters involved did a lot of their own oversight before those stories were published. And if you kind of look at the chronology, which I was tasked with providing, basically the stories started when Snowden talked to a documentary maker named Poitras, who was friends with Glenn Greenwald of the Guardian and Bart Gellman of The Washington Post. Greenwald then started a long series of contacts with Snowden and in the end spent a week with him in Hong Kong interviewing and getting the data for his Guardian piece, which appeared in early June, on June 4th, in fact, saying that the court had ordered Verizon to turn over millions of records on U.S. customers.

A few days later Bart Gellman of The Washington Post, who had also been in contact with Snowden, broke the story about PRISM, which is a database that allows the NSA to access a variety of communications from nine of the big Internet providers.

They also published some slides saying that the NSA had direct access to providers' servers. However, that has been denied by the companies and disputed by other media organizations, and The Washington Post has rolled back on that story, saying there – there's direct – maybe was misunderstood and that in fact what it seems to do – and some of my colleagues can speak more to this – is that barrages, basically, of information are provided in response to court orders, and the NSA is then getting that information direct from companies, as opposed to intercepting communications that are kind of going past them. But I think The Post did have to roll back on that, and it probably shows that journalists need to have a better understanding of what data collection is really about. And I think we're going to talk a little bit about big data later. It's an area that journalists certainly need to have a better understanding of that.

After those articles, as you probably all know, Snowden revealed himself as the source in a video interview with Glenn Greenwald, and that's kind of unusual for a whistleblower, actually. Usually they stay behind the scenes, but it really has changed the dynamic of this story. Then, of course, he disappeared and continues to be sought after by the government.

MR. RISHIKOF: I mean, I guess the question is, is that, you know, there's a whistleblower statute. There's a difference between a whistleblower and a leaker; a leaker a source kind of in the terminology.

But I guess for you and Gene, what about the philosophical view? I've had situations in which documents have been inadvertently leaked to the press. The press has come to us and talked about whether or not this would really hurt the government. We've told them it's going to really hurt the government. And some of the press have said that we're not going to go with this story because we realize what the consequences are going to be for the United States government. So I think it's a bigger sort of question about (on what is ?) journalism. And so if you and Gene – Gene, do you want to take that and we'll have Ellen respond.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

MS. SHEARER: Go ahead.

MR. POLICINSKI: Well, I think, again, let's sort of try to set this in a larger perspective. And I've listened to the very valuable and, I think, very accurate descriptions of the programs, and I'm glad to see that additional information is coming out because I think ultimately that is the – you know, the words that we don't often hear, which is national security and transparency. Those are not incompatible, but they are often issues which start out as sort of different sides of the table, and they have to meet somewhere.

But, you know, history's replete with examples where news organizations have not – and sometimes to their regret – published information that they had which classified or secret. I think it was Ben Bradlee who said if the Post had published about the Bay of Pigs, we might not have had that incident. But you can go back to Gary Powers and the U2 – known for a year before – U2 program – knowledge about the U2 program in 1960 was known before Gary Powers was shot down.

You can march through a number of programs: the CIA detention program. You can talk about some of the disclosures of data collection or other techniques to deal with terror that have been withheld. A very common practice for journalists is to consult with government officials prior to the time and withhold all or part of information. That's a system that's been going on for quite some time now, at least again in sort of modern-era 40-some years.

You know, and none of this collision is new. I've been joking, but in all seriousness, you can trace it back to the XYZ Affair in 1797. You know, it was seven – six years after we passed the Bill of Rights. There's a move by the United States to deal with France. Diplomats go over. There's some allegations about bribes. That's been disclosed, and (I worry ?) about the consequences here because a year later we passed the Sedition Act and editors are being jailed. We can march through history with a number of those examples.

But I think what we have here, if you can back up a little bit from the specifics, Harvey, is if you look at it from the American people, you have what I think everyone here is making out the point is not a monolithic national security structure in which there's sort of a one order and everything goes through. There's a lot of review and back and forth. But you know, the American people are presenting with a system periodically which appears to be monolithic because it is silent. And uncharitably, perhaps, to use some of the explanations today, we're now confronted with a system in which there is a haystack gathered which apparently can be accessed by a rogue farmer, contrary to all the rules and regulations that are set up, with information straws pulled out at – to some degree at random or with a purpose, to do harm to individuals or the nation. So



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

if – you know, I understand and I really do appreciate in a very real way the checks and balances setup, but I think when you look at the role of a journalist here, the founders set us up outside of this structure of independent – of checks and balances within there to be that independent check. And I don't think it's quite fair – although – and again, the journalists involved here could either defend themselves or not to someone's satisfaction or not, and that's their job, not mine. But I think we have to say, we did set up this system with a group outside of all of these checks and balances to be able to say, wait a minute. Let's look at this from a larger point of view. And I also don't think that there's ever been a death attributable to that information being disclosed – that I could find – a single death attributed to the disclosure of those kinds of information. And that may be a game changer. I think as our first speaker pointed out, that may be a game changer in how the role of the press is evaluated.

MR. RISHIKOF: So Ellen and then –

MS. SHEARER: Yeah, and to kind of get back to the more specifics, I will I think defend the journalist in this case in that there was not a rush to publish. They spent time – they did contact government officials in advance to say that they have this information. And they also didn't publish everything they had. They had more slides than appeared in the newspapers. So, you know, I do think it's important to say that journalists do understand the nature of the information they're dealing with and over – you know, over time it's often the case that either they've held back information that the government asked them to or that in their own judgment was too sensitive to share.

MR. RISHIKOF: Well, Spike, I want to get you in here because – and we'll go back to the journalism issue, but you're probably (one of ?) the few people that's actually before the FISA court and actually argued in front of them. And I was just curious if you could talk about your understanding of that experience as to – as people have been saying, it's a rubber stamp versus an actual court that actually puts the government to the test for its evidence.

MARION "SPIKE" BOWMAN: Well, we're talking about NSA programs here. And many years ago as a uniformed officer I was assigned to the National Security Agency, became exposed to FISA there, the Foreign Intelligence Surveillance Act, but I did not actually have anything to do with it. My very good friend Mike Smith (sp), who is sitting in the audience here, was the one who actually did it at NSA.

But the function we're talking about here is oversight of the – of the court and for what purpose is the oversight. And I spent a number of years at the Federal Bureau of Investigation. We used – working with FISA on a daily basis. I've worked through many thousands of FISA applications, and I have a very good view of what the FISA court does.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

Now, I have heard for years that the FISA court is a rubber stamp because so many are actually – so many FISA applications are finally rejected. It is true that not very many FISA applications are rejected. Let me explain why. First of all – and I'm going to use the example of the FBI primarily here because the FBI first of all focuses almost 95 percent of all of their FISA are on persons. So that's where the biggest issues of privacy are going to arise.

The judges of the FISA court are all senior judges that have a great deal of experience in other walks of law. They're appointed relatively far into their career as federal judges. They come in for seven-year terms, staggered terms. There are 11 of them. And so there is always a judge rotating off the court.

And when they come into the court – and I don't mean to be facetious here, but the judges generally can't spell the word "secret." They are – they have never been exposed to the – to this type of activity before. And frankly, they come in suspicious. Like most Americans, federal judges are suspicious of secret activities. They also come in with a broad background in protecting the rights of privacy for Americans or for their – the targets of their – of criminal warrants. And so they're very used to the idea of having to look at the secrecy and compare it to the privacy issues of Americans. And so they – as I say, they come in, and first of all, they're very suspicious. So that's one way – one thing to keep in mind.

The other thing to keep in mind is how the FISA application gets there. And it's much more convoluted for the FBI than it is for the National Security Agency. So again, I'll use the FBI because the hardest process to come – coming through. The application begins somewhere in the field. You know, it doesn't start in Washington, D.C., where the court sits. So first of all, that's a different experience for the judge. He's used to having a –

MR. LITT: Can you make clear what kind of FISA you're talking about here? Because I – we didn't talk about that earlier, and it might be useful to explain that.

MR. BOWMAN: OK. The – at the present time I'm talking about the – a FISA application to target a person. So that makes a difference here. But the point of the matter is that the judges are focused on privacy from the day they walk into this new office they've got. And so they're looking at privacy issues for the 215 program and for the 702 program as well.

But the application starts in the field, the application goes to the headquarters of the Federal Bureau of Investigation, where it must be approved there by operators; it's already been approved by an operator, a significant administrator and a lawyer in the field. When it gets to the headquarters, it has to be approved by the supervisors there, then it goes to the lawyers at the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

FBI, where it has to be approved by at least two lawyers there. It then goes to the Department of Justice, where at least three more lawyers will look at it.

Now, I will tell you, in approximately 70 percent, maybe 80 percent of the cases that application is going to be sent back at at least one of those stops along the road for more information, for more justification. Many of them are sent back several times. When it finally gets to the court, the court is now looking at something that, as I said, is really beyond their normal experience and they are suspicious of secrecy and they are concerned about privacy. And the court will ask questions and frequently, very frequently, they will – they will hold a FISA application to make sure they understand what is going on and to get more information to them. I've seen FISA applications held over for months at a time to make sure that the applications are properly prepared and that there is no issue of privacy that would trump over the issue of national security.

MR. RISHIKOF: Thank you, Spike.

You know, lawyers just love process and procedure, and I think there's nothing we enjoy more than getting in front of judges and having to justify ourselves. (Chuckles.)

So let me –

(UNCLEAR): Harvey, not only held, but kicked back.

MR. RISHIKOF: And kicked – but the key is kicked back.

Let me – I had a tweet and a question and I'm going to combine them, because I think it sort of reflects the concern. So the combination is that it's clear in the government, though, that we have different types of data that exist. We talk about telephones, we talk about emails, we talk about metadata, and we talk about electronic communications.

This is all sort of zeros and ones now as we move into the digital age. The historic statutes that were tied to different types of technology are truly changing. And the question for you guys as a group, and I'll start with Bob, is that A, We are collecting different types of information and putting it together and then we're banging that information. And no one really expected the ability to do that the way we are able to do it now, and is that somehow changing the relationship of the government to individuals? And what is the process in the rules and regs, putting all different types of information together, legitimately acquired by legitimate different parts of the state and then put in a basket, banged and then given back to different parts of the state? Should we be OK with that?



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

And the second question is – that's tied to that is once you're looking for criminal – once you're looking for the terrorist activity, if you stumble across some criminal activity in the data, what's going to be the response of the government if they see that criminal activity, though it may not be tied per se to terrorism?

So let me start with Bob, he can respond to that and the general issues that have been put forward.

MR. LITT: So I think I'm going to not answer the first question, just because I think as posed, it's really too vague to admit of an easy answer.

What I can do is talk a little bit about process again, which is to say that we think about these issues all the time. The FISA court thinks about them when we go for FISA court applications. We have – in the Office of the Director of National Intelligence, we have a Civil Liberties Protection Officer who thinks about these issues all the time. The President's Intelligence Advisory Board and the PCLOB think about them all the time, and the Congress thinks about them all the time. And I think they're worth talking about and thinking about.

Kate raised the question of whether the standard Fourth Amendment law about no expectation of privacy in information that you voluntarily expose to third parties, whether that law ought to continue. That's a debate that's worth having. It is the law now, however, and we make use of that authority.

On your – what was your second question? I forgot, Harvey.

MR. RISHIKOF: Sort of where – what happens in the event that –

MR. LITT: Oh yeah –

MR. RISHIKOF: – if you come across something that is not tied directly to terrorism, but when you actually start looking at the content under 215, you may find something?

MR. LITT: So the statute and the orders allow us to disseminate information if it's evidence of a crime. I actually think that most people would agree that's probably the right policy decision. If you come across – if – criminal activity, and it's information that you've lawfully collected, are we really comfortable with saying, oh, just stick that in the trash, because it doesn't relate to terrorism? I don't think that's the right result as a nation, and generally speaking, it's not the result that we have with other kinds of data.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

That doesn't mean you can look through the data for that; you have to be looking through the data for a foreign intelligence purpose.

MR. RISHIKOF: Does anyone else want to pick that up?

MR. BRENNER: Let me take a crack at the first question.

MR. RISHIKOF: OK.

MR. BRENNER: The – we live in a sea of data now. We – I think all of us have – are beginning to understand that. Where we shop, what we buy, the patterns of our commuting, when we get on and off the subway here in the – you know, with one of these cards that makes a record of where we clock into the Metro, when we get on the bus, when we drive our car across – through a tollbooth – we leave electronic footprints to an extraordinary degree. This is – that fact, that sea of data that we are swimming in is certainly changing our relationships across the board, not just with the government. It's changed our relationship within our families, to our families and our neighbors, with our – the places we shop.

Right now there are people in the private sector who are taking information from Facebook and Twitter and so on and matching the – doing the sort of analysis – the link analysis of – and showing networks and matching it with other networks and coming up with extraordinarily rich data about us, whether we like it or not. The difference is that we have rules about how the government can do it that are really strict. So in answer to that question, yeah, it's – it could change our relationship with our government much more radically than we want to. That's why we have the kind of rules that Bob laid out that restrict the government's ability to look at this stuff.

MR. RISHIKOF: Well, Gene, and then –

MR. POLICINSKI: Well, you know, I think sort of underlying some of this is a sort of a question being raised by those in government about why – you know, why there was such a need to disclose this, you know, almost a what's – you know, what's the rush? What's the interest here? And I think if we look at this, we really have three separate issues bringing up, two of which are very much in this group, which – in terms of the government, which is the validity of the – of the process of the internal review, which is FISA courts and the internal checks and balances, and then the scope of the programs in law. And those are – those are two really Washington kind of based things.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

But then we go to the larger thing, and I think that's prompted the public's interest and is driving some of the journalistic interest in this, and this is really the public discussion of the concept of big data, data collection, almost without regard – although the stories broke – with regard to sources and methods, but almost without regard to that. And that is this thing – you know, in 1890 there was a tome here that – by Warren and Justice Brandeis, so eventually Justice Brandeis talked about the right to privacy and defined very simply the right to be let alone.

And I think what's resonated with Americans here is not so much a debate over the – you know, those first two parts of the discussion, which are very important, but it's that third part that is attracting attention and I think will ultimately become the larger debate, as you've pointed out, which is this right to be let alone, this right to have data not collected in the big haystack, the right to – maybe to have these programs, or the need, rather, to have these programs focused. I think Senator Leahy is proposing some legislation to tie some of the collection to specific needs. I don't know if that's possible or not.

MR. RISHIKOF: I don't want to get Stewart excited, but this comes to data storage issues, and so the European approach versus the American approach is quite – but I know that Kate wanted to – (off mic) – Kate, what did you want to say?

MS. MARTIN: Well, I just want to agree that what I think's changed is that we used to have two protections against government overreach. One was the law, and the other one was that the government didn't have the capability of – to know everything about us. We've lost the second one, so we have only the law. And while I've devoted my life to the law, I'm actually more skeptical that the three branches of government, when acting in secret, really are going to be able to make sure that the law makes sense and it's being followed.

And just quickly to mention the fact that in the last 10 years we had an example of the government issuing, in secret, a legal opinion binding on the whole government to the effect that the president had the power to violate whatever law he thought needed to be violated in the – in – for national security purposes, and do so in secret.

Now, the way that was revealed was through the press. And I think the essential constitutional structure of oversight, which is the three branches, includes the press. And the fact of the matter is for all of us who deal with the Congress – the Congress, and also the courts, to some degree – their agenda, their understandings are vastly influenced by what's in the press.

And to say that all of this is going on – and so I'm not questioning whether or not they aren't – I'm sure that Bob's informed them when he's found errors. I think it's a much larger question



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

and a much larger problem. I think if we have a vice president who thinks that it makes sense for the government to change – to violate the law for national security purposes, the question is, what kind of robust system do we have to stop that?

MR. BAKER: So two thoughts. One, we don't have a press anymore. You can see the future from here. We have a host of bloggers, a host of people with attitude.

MS. SHEARER: (Off mic) – you're one, but –

MR. BAKER: This story went to Greenwald – Glenn Greenwald because he had an attitude. And I am one. Yes, that's right. I'm as much a journalist as Glenn Greenwald. God help us all. I –

MR. POLICINSKI: Well, and under the First Amendment, that's exactly right.

MS. SHEARER: Yeah. That's – exactly.

MR. BAKER: That's quite right. And so to the notion that there's some institutional gray lady who will be responsible and thoughtful about this and tell us what we need to know but only what we need to know, I think it's over. And I – this tell us it's over. And I can't trust these stories. You know, it was Bart Gellman's story. What was new in that story wasn't true and what was true wasn't new. And it was – it was a stampeding kind of story. I – and so that's point one.

Point two, on this question of, you know, the right to be left alone, I think you read that article closely, what Justice Brandeis was really saying is he wanted a right not to have this newfangled thing called Kodak photography used against him.

MR. POLICINSKI: And the telephone, I believe, right? Yeah.

MR. BAKER: Right? Because he was deeply uncomfortable with what that meant for his prior sense of privacy. We're all familiar with that experience. I – the first time you read the Google results on yourself you kind of get it. (Laughter.) I –

MR. LITT: Stewart, you really Google yourself? (Laughter.) It's OK.

(Cross talk.)

MR. BAKER: Can I just – but the point here is the technology is moving. It makes government



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

more effective. It also provides protections that were not previously available for privacy. I mean, you can guarantee the government can't wiretap you with secure encryption. The idea that we should say the government and only the government can't have these technologies, can't take advantage of technologies, is not going to work.

(UNCLEAR): Yeah, so let me – let me interrupt –

((UNCLEAR): Well, I don't think that's the –

MR. RISHIKOF: Let me just sort of focus the group, which is that, first of all, if you look at the Supreme Court Justice Brandeis' official painting you will see he had a bit of a hair issue, which is, I think, why he was so worried about the – (inaudible). (Laughter.)

But the question that really comes to the fore in this issue, which is also coming from the tweet and the crowd, is that – the first question is sort of a legal question, is why isn't Sanders – I mean, Snowden going to be under the whistleblower protection? Because he didn't follow the whistleblower statute to do what he had to do. There's procedures – there's procedures are done.

But more specifically, part of this issue which you are raising is the relation of journalism and activists. And the question is, are there any legal issues when – with journalists actively persuading someone with a top secret clearance to leak information and then getting involved in the process of the story.

MR. POLICINSKI: I knew we'd come around to the Espionage Act at some point.

(UNCLEAR): OK, right. All right –

MR. RISHIKOF: So I think – that's what I think raises people's sense of what a traditional journalist does, what an activist does, and then – what – how you become involved in aiding and abetting or a conspiracy to violate laws. That's sort of the two – the issues I think people are raising in this – with this particular case and the future.

MS. SHEARER: Right. Right. Well, first of all, advocacy journalism has a long tradition in this country. In recent times, we – you know, the mainstream media has been less advocacy journalism and more objective reporting, would be the criteria that we would use. But you know, Glenn Greenwald is a columnist. And he absolutely has a point of view. That doesn't mean he's not a journalist and that doesn't mean that the information is not accurate. You can have a point of view and be accurate, you just have to –



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

MR. BAKER: It wasn't. It wasn't.

MS. SHEARER: Well, I think –

MR. BAKER: He's entitled to be inaccurate as well.

MS. SHEARER: Yes, he is, in fact. But I would argue that it wasn't –

(UNCLEAR): Well –

MS. SHEARER: You know, we're going to have to agree to disagree on that. But you know, the fact that he had a point of view is fine. You know, as long he's labeling and telling his audience that he's coming at a certain point.

Now, in terms of enticing people to give you information that they weren't planning on, that isn't actually, to my understanding – and I don't know Mr. Greenwald or Bart Gellman personally, but my understanding is Mr. Snowden came to them, basically, with the information, and they were – you know, again, they reviewed it, they, you know, tried to determine its accuracy, and they determined which parts were, in their minds, fair. And I would disagree that the future of journalism is dead. (Chuckles.) As a journalism professor, I have to disagree – (laughter) – and in fact, I do disagree.

MR. RISHIKOF: Well, there's a tenure issue involved. (Laughter.)

MS. SHEARER: But you know, I do think you're right that when you're blogging, you're a journalist, and you have a point of view. The main point for journalists is just – maybe like for the government, transparency. You know, if I have a point of view, I need to tell you that I have a point of view. But even if I have a point of view, as a journalist – and I think this is true with Mr. Greenwald – you know, I still should not be just distorting or withholding pertinent information to make my case. I have to still be fair even with a point of view, and I certainly think you are in your blog. (Laughter.)

MR. POLICINSKI: And just to carry it a little bit further on, I think, again, this is another one of these sort of oil and water issues. The process that is set up here and been described, again, I think, very ably about checks and balances within a system is checks and balances, checks and balances, checks and balances, result. And I think what we're seeing here, and even in the change-over from media establishment, you might say, or traditional media, to this new world of everybody, you, me, everybody getting access, is almost a result, then correction, correction,



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

addition, call to account. It is going to be a very different system than we may feel comfortable with. But I think we're, collectively, the FISA Court process. We are, collectively, the review process. If you in fact can demonstrate that these guys wrote something that's not right, you now have access, from your house, in your blog, to the planet.

MR. BAKER: In my slippers.

MR. POLICINSKI: In your slippers – (laughter) – bunny slippers in some case – you know, in some people. But I mean, you do. You know, there is an accountability aspect here that the profession – the Fourth Estate is not without, because is the court – in the court of not just public opinion but public review. And they can be held accountable in a fashion that the founders, I think, envisioned, again, by setting up this structure in which there was this independent press that could be called to account by others. You know, the First Amendment protects the right to publish. The First Amendment protects the right to speak. It does not shield you from criticism, from being called to account. So I think it's very important to say that, you know, it's not an unleashed, unaccountable structure here. And I think that's one of the issues here. When we talk about the responsible organizations talking to government in advance, again, we're replete with examples where people do vet information.

MR. BRENNER: I got really – I mean, I disagree, Gene. There are two things going on here that I think need to be proven out. One is that information is now extraordinarily difficult to control, which is why we are seeing, not only in our personal lives but in our corporate lives and in our government, a degree of transparency that none of us grew up with. We talk about secrecy going through the roof, but this event shows how hard it is to keep anything secret.

The second thing is that the press – and you would call the responsible press – is not just an American press anymore. We are now seeing the internationalization of these issues. And there is no accountability in the sense that we – again, that we – that we grew up with. We are talking now, in the case of Snowden – and let's pull apart the disclosures relating to the government programs, where we could have a debate about what should be public, what not, with what else this fellow has put out there. I mean, this guy has done us tremendous damage. We are now dealing with a penetration agent that is somebody who went to work for Booz Allen knowing he would get access to NSA in order to steal secrets, and we may be dealing with the first penetration agent in history on behalf of a private organization. This remains to come out. We don't know that yet.

And that guy is now in – the South China Morning Post and The Guardian are not going to be talking to the president of the United States, the attorney general about what's going to do us harm or not. They may be quite happy to do us harm. This guy has let out information about our



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

collection against certain foreign diplomats. He didn't tell the Russians – the Russians knew that – because they do it, right? They do it. What he told them is that we can collect their stuff. We're going to lose that access. He's done us tremendous harm, tremendous harm. This is a guy who's set out to hurt the United States. Shouldn't be – shouldn't lose sight of that.

MR. POLICINSKI: And I – and I'm – again, you know, the accuracy of these stories – and the damage – again, I will concede –

MR. BRENNER: I'm not talking journalistic issues here. I'm talking about who this guy is.

MR. POLICINSKI: No, but you're – but you're putting a tinge on that. And where was the failure? The failure – The Washington Post didn't hire Snowden. The Washington Post didn't vet or The Guardian didn't vet this young man. I mean, there's a failure here – if there's a failure in terms of the control or regulatory aspect of the – and the access to data, that doesn't rest with the reporters who ultimately produce the information.

MR. BRENNER: Well, you don't have to defend them. I'm not attacking them.

MR. POLICINSKI: Yeah.

MR. BRENNER: I'm talking about – I'm trying to talk about – let's separate the different kinds of baskets of information that have been put before us because they're very different.

MR. POLICINSKI: They're very different.

MR. RISHIKOF: Kate?

MS. MARTIN: So I agree that they're very different. But I want to suggest a different question, which is, is there an issue here about the secrecy of the U.S. government about surveillance programs directed at its own citizens? Which there is a pretty good likelihood we're going to come out sooner or later someday, and the consequences of them being made public in this way instead of the way which we've been urging them to be made public, which was an answer to congressional request, et cetera, is – (applause) – (chuckles) – is – I mean, so the consequences include world public opinion thinks the United States is a hypocrite, which matters for all kinds of national security reasons. It means that the United States is in a much more difficult position to object when foreign governments really do spy on their political opponents, which does happen, and the U.S. has been the kind of, that's against the law and against human rights; it's much harder for us to make that case. And I assume that the negotiations between the United States and China on doing something about cybersecurity are



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

really in a mess because of this. And yes, Snowden is the proximate cause, as we say in law school, and those were all terrible consequences. But I do think that when you organize the government around the question of secrecy, et cetera, you in this day and age need to take into account the fact that the people are going to say, we have a right to know this stuff, you need to tell us, and – unless you're really, you know – and you – it's going to be really hard to prevent it from coming out.

MR. RISHIKOF: One of the questions from the audience is that it's clear there's been a lot of oversight, and we've referred to the idea that when there's not compliance, that the government acts to enforce that compliance. Then with this – from Lawfare (lawfareblog.com), who's – they're streaming it live on Lawfare, was sort of focused on how often you had noncompliance, and you guys would know that experience, but that there is a system in there that's trying to find it.

But the other interesting question is, is that some individual is allowed to get on the system and remove these documents, and we didn't know that until they became public. So that's a problem, I think, from the government's perspective, that that was able to happen despite an alleged, very extensive oversight system. So the assumption is I guess we're going to have more of an oversight system to make sure these individuals will have this type of IT power inside the new big data will be watched even more closely.

So A, what's your sense, Bob, about that, and how do you all feel about the idea of that sort of the new nuclear scientists of the 21st century are the – our IT people, not the people who used to make the bomb? This is – how many people in the audience know how to write an algorithm?

(UNCLEAR): I do, but – (inaudible) – computer. (Chuckles.)

(UNCLEAR): Oh, my.

MR. RISHIKOF: Unfortunately, those people who know how to do it are the ones we call sort of the value-added now in the big-data era.

So what is your response to that issue about how the governments can respond and how you all feel about what the effect that's going to have on law and policy over the next decade?

MR. LITT: So I have two comments. The first is to make very clear that the – Snowden did not take data from the kind of database that I'm talking about here. There is – there is a set of sort of, you know, system that the NSA uses to run its business. That's where he got this stuff from – allegedly, I guess I have to say. But there is no indication that he was able to penetrate the



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

databases on which this actual data is maintained.

Having said that, yes, we need to go back and look at the systems, whether we can impose more restrictions on them. I think General Alexander, who's the head of NSA, has already indicated that he's looking, for example, at a sort of dual key system for system administrators.

The fact of the matter is that ultimately it all depends on trust, and if there's somebody who's willing to violate their trust, it's frequently hard to prevent it from happening. We can do everything we can, but we are always going to live with the reality that there are going to – people who are going to be faithless.

MR. RISHIKOF: I know it's hard to imagine, but the hour and a half has flown by. Does anyone have a last comment they'd like to make? Bob or Ellen? (Pause.)

OK. Let me just say that it's – I want to thank everyone for, I think, a very, very fascinating and informative debate. We'll be able to view the program again on the ABA website, which is www.americanbar.org/natsecurity.

Again, www.americanbar.org/nationalsecurity.

If you'd like to receive future notices of programs such as this one, please send your email address to the contact link on our website.

I want to call your attention to three books that we have that are on – for sale. The first is the – “National Security Law in the News,” which I highly recommend, which goes through many, many areas of the national security law and how journalism interact. A number of people on the panel have written actually chapters and it's extremely informative.

We have another book, called “Patriots Debate,” which looks at contemporary issues in national security, and then “National Security Law: Fifty Years of Transformation.” I think Jill Rhodes is in the audience, and she – it's another book that sort of lays out the big issues.

But I think – I'm going to just quote from the Constitution. I think there's a tension, and the tension is there, and I – that's why I think we're going to continue to have more debates about this area, because the Newseum is famous for the – protecting the First Amendment and, they like to say, the five freedoms. I could call on someone to ask them what the five freedoms of the First Amendment are, but we all know it'd be slightly embarrassing. So I'll just read what the five freedoms are of the First Amendment.



Transcript: Newseum Special Program - NSA Surveillance Leaks: Facts and Fiction

MR. POLICINSKI: Bless you.

MR. RISHIKOF: They are “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people preferably – peaceably to assemble, and to petition the government for a redress of grievances.”

But the tension is Article 1, Section 5. Article 1, Section 5, is very rarely read, but it’s read by people who are in the intelligence business and the Congress. Article 1, Section 5, says, “Each house shall keep a journal of its proceedings, and from time to time publish the same, excepting such parts as may in their judgment require secrecy” – secrecy’s actually mentioned in the Constitution, and privacy is not – “and the yeas and nays of the members of either house on any question shall, at the desire of one fifth of those present, be entered on the journal.”

The Congress is really the focus of understanding where secrecy should be. The executive branch has its perspective, and the judiciary has its, but the Congress is really, I think, where the center of gravity is.

And what I hope that – is that you enjoyed this particular event, and I’m looking forward to more ABA Newseum events in which we actually explore these issues in such a mature, thoughtful way. I think we had more light than heat, which is what really one focuses for. And I again want to thank the Newseum, Medill, and the McCormick Foundation for supporting this, and I particularly would like you to join me in thanking our panelists, who I think were extremely enlightening and helpful this afternoon. (Applause.)

So that ends the proceedings, and I look forward to seeing some of you later. But I want to thank you again for taking time and doing this.

(END)