Intelligence to Protect the Homeland Symposium

"The Evolving Terrorist Threat and the Importance of Intelligence to Protect the Homeland"

Co-Hosts: Intelligence and National Security Alliance & the Center for Strategic and International Studies

Civil Liberties and Security Panel

Introduction:

Colonel (ret.) Joseph D. Rozek, Senior Associate (Non-Resident), Homeland Security and Counterterrorism Program, Center for Strategic and International Studies

Speakers:

Matthew Olsen, Director, National Counterterrorism Center

Chief Cathy Lanier, Washington, D.C. Metropolitan Police Department

John Pistole, Administrator, Transportation Security Administration

Suzanne Spaulding, Principal, Bingham Consulting Group

Moderator: Jeanne Meserve, CNN Homeland Security Correspondent

Ronald Reagan Building & International Trade Center
Washington, D.C.

September 7, 2011

COLONEL (RET.) JOE ROZEK: Good afternoon. We're going to start to, this afternoon, with some panels. We'll wind up with the director of national intelligence.

But before we do that – this is the best part of the day for me – a year ago, there were about 70 people got together and started working on a project called, let's define Homeland Security Intelligence Enterprise. Well, that was whittled down to 40 people when we got into that four-letter word called "work."

Now, these 40 Americans, 40-some Americans, I characterize as great patriots. These are people from academia, the public sector and private sector, who had day jobs, but at night, on weekends and holidays, met to discuss the issues, to frame the issues, to listen to people talk to us presenters. They wrote. They would take it to the – they'd take their papers to the advisory boards, the Governance Board and the special advisers and get critiqued and go back and write again and write again and again, to present today what you have as the paper outside on the table.

In addition to this paper, the Intelligence to Protect the Homeland, there are three additional papers that will be posted online in the short term and a fourth later on.

So I think it's only appropriate now that we recognize those great patriots who, in true American spirit, were not satisfied with the – with the status quo, but took on a tough challenge to define what we have known to be but never recognized, the Homeland Security Intelligence Enterprise.

I'd like to start off by recognizing my two co-chairs, the vice chairs, Dr. Kathleen Kiernan and Dr. Laura Manning Johnson. Please come out on stage. (Applause.)

We also had a dedicated intern. She doesn't expect to come out on the stage, but I want her to come out here. Miss Amanda (sp). (Applause.)

I'm going to recognize – I want you to hold your applause – I'm going to recognize four – there's five, two co-chairs for one committee and three other chairs – for the subcommittees, I mean.

First, subcommittee one, the definition, Rob Rigo (ph) and Neil Schlum (ph); please stand up if you're here. I know Rob (sp) was here earlier but might have left.

The second subcommittee, which is development integration of the Homeland Security Intelligence Enterprise and public engagement, Mike Rawlins (ph).

The third subcommittee, full integration enterprise and ecosystem, Michelle Farr (ph).

And the fourth subcommittee, the privacy and civil liberties mission, Dan Parito (ph).

Now, with that, would all – stand up – keep standing, Dan (ph) – will all remain – all the other members of the Homeland Security Council for – Homeland Security Intelligence Council,

please stand up; the Governance Board and special advisers and all the INSA members who helped us out, please stand up and please give them a round of applause. (Applause.)

These are true American patriots.

I turn it over to Kathleen.

KATHLEEN KIERNAN: It's always both humbling and rewarding to follow a guy like Joe Rozek. Col. Rozek epitomizes in my mind everything that we should – we should strive to be as leaders, quietly competent and sincerely a genuine American hero who's absolutely a pleasure to work with and serve Joe.

I have the pleasure now of introducing just a dynamite panel. And let me start with Matt Olsen, newly appointed director of the National Counterterrorism Center – and had the opportunity, as the newly appointed director of the National Counterterrorism Center, to brief the president yesterday, which was pretty exciting, I understand. He's former general counsel of the National Security Agency, former official at the Department of Justice, a graduate of Harvard Law School and a professor of law at Georgetown University.

Next to Matt is Chief Cathy Lanier of the Washington Metropolitan Police Department. Cathy earned her bones in the street beginning in 1990. She was part of and led all aspects of the uniformed patrol and tactical operations with the police department. Cathy also represents the very best America has to offer in the law enforcement world. She holds dual master's from Johns Hopkins University and the Naval Postgraduate School.

Next is John Pistole, currently the administrator of the TSA following a tremendous career in federal law enforcement with the FBI, earning the rank – and earning is much more important than being appointed – earning the rank of deputy director. Under his watch, TSA continues to grow as a risk-based, intelligence-driven counterterrorism agency dedicated to protecting our transportation systems. John also has a law degree from Indiana University School of Law.

Next is Suzanne Spaulding. She is recognized around the world as an authority on national and homeland security issues, including cyber, critical infrastructure, CBRN weapons. She served as the minority staff director of the HPSCI and also as the general counsel for the SSCI. She was the assistant general counsel for the CIA prior to that and she currently works in the field as a practicing attorney.

This panel will be led today by Jeanne Meserve. And when I was thinking through her career, I had to draw a parallel to law enforcement. Investigative journalists have a kindred spirit with law enforcement officers. They see the world through untinted glasses. They speak the unvarnished truth and seek always to examine the most complex of issues.

Please welcome a highly acclaimed anchor and reporter and a woman used to driving world change in a marvelous panel. Thank you.

JEANNE MESERVE: Kathleen, thank you. (Applause.)

Thank you all. So Scott McNealy of Sun Microsystems said a few years ago, you have zero privacy; get over it.

Now, I don't think even the most zealous civil liberties advocates really think we have zero privacy, but certainly they have concerns that civil liberties and privacies have eroded since 9/11 with the Patriot Act and more today. Hopefully, we're going to get a fix on where we are, where we might be able to improve, where things should change.

So first, I'd like to ask each of our panelists to set the stage from where they sit. Mr. Olsen, this is your first appearance of this kind since becoming head of the NCTC, so let me let you do the honors here with your remarks first.

MATTHEW OLSEN: All right. Thank you very much, Jeanne. And thank you to INSA for holding this panel. And it's really an honor for me to be participating in this with my friends and colleagues. We represent a sort of a – I was thinking about – we represent a number of perspectives, federal, state, local law enforcement intelligence, and I think it's a very fitting group, along with the private sector.

So, yeah, I've been at NCTC for all of about three weeks. I walked in to lunch a little bit late just in time to hear General Hayden say NCTC was an unqualified success. So I almost thought I'd just get up and go home; my part was done. (Laughter.) But I can't take credit for that. Mike Leiter, my predecessor, Admiral Redd before him, and John Brennan, who helped start the whole thing going, deserve the credit for that. But I hope to continue that record of success.

So I'll just say a couple words about NCTC, what our mission is, and then a couple of quick thoughts about the privacy and civil liberties issues that we face.

You know, first of all, as most of you know, NCTC was created post-9/11; it was a creature that – of that tragic day. It grew out of the work of the 9/11 Commission, and then Congress in 2004 created NCTC.

We really help lead the government's efforts to combat international terrorism. We combine people from around the intelligence community and outside the intelligence community in a really healthy and diverse mix of professionals who bring a varied set of perspectives and backgrounds to look at all the information that we can bring together. And we are singularly focused on that one mission, which is counterterrorism.

So very briefly, just a couple of our mission sets: One is intelligence analysis. By law, NCTC serves as the primary organization in the U.S. government for analyzing and integrating all intelligence about terrorism and counterterrorism. We have a unique responsibility to examine international terrorism issues that span geographic boundaries. We analyze intelligence regardless of where it is collected, whether that's inside or outside the United States, and we

have access to essentially the entire catalog of counterterrorism information that the government possesses.

Our second primary mission area is watch-listing. We serve as the central and shared knowledge bank on known and suspected terrorists. And we support terrorist watch-listing. We maintain the Terrorist Identities Datamart Environment, or TIDE, that many of you have heard about.

Third – a third mission area or responsibility I'd like to highlight is – and I think it's particularly relevant to this panel – is sharing information with state and local law enforcement. We have a group called the interagency threat assessment and coordination group. But in a nutshell, it's a – it's a small group of professional first responders from around the country who come and serve at NCTC, led by DHS and FBI, and their responsibility is to look at all the intelligence that we are producing and seeing, and to take that information and turn it into products for first responders. So we have a product called Roll Call; unclassified piece of analysis that is designed specifically for a first-responder audience. And that goes to the issue – again, that General Hayden talked about – of not just vertical intelligence but horizontal – I'm sorry, vertical sharing of intelligence down to the state and local – our state and local partners.

The fourth area of responsibility I wanted to highlight is our strategic operational planning. And this is a little bit different than the others in that it's not part of the intelligence community per se. But in this response – in this role, we are charged with conducting strategic planning for counterterrorism activities. We work closely with the national security staff at the White House to support a wide range of plans, both strategic plans and implementation plans.

So very briefly, two quick points I wanted to make when I thought about this panel with respect to privacy and civil liberties:

The first is that these two goals, national security and privacy, are not in conflict in the way that people, I think, often think they are. From the perspective of NCTC, from my time at NSA, we have to – we must do both of those things. And we can do both of those things; we can achieve greater security without any sacrifice of privacy through policies and technology and practices.

And then, just finally, I would want to share that I do – have been very impressed – I am an attorney by background – I've been very impressed so far with NCTC's record of privacy protection in my first few weeks.

MS. MESERVE: OK. Suzanne, why don't you take it next? Just quick thoughts on this issue of privacy and security.

SUZANNE SPAULDING: All right, well, I want to pick up on Matt's last point, which is this notion that I think, well, you'll hear, I suspect, from everybody up here, which is reflected in INSA's report on civil liberties, that we need to stop to thinking of these as mutually exclusive values. And I think one of the ways to do that is to watch – pay attention to the way we talk about it.

One of the things that has kept us from really understanding the relationship between these two is our traditional way of talking about balancing national security and civil liberties as if they were mutually exclusive objectives on opposite sides of the scale. And if you just took away from one, you'd add to the other and vice versa, when in fact they are mutually reinforcing.

We all understand that security is an essential framework within which to protect our civil liberties, but it is equally true that civil liberties really are a great source of our national security – obviously, a source of our strength, but important for national security.

And we've heard some specifics about that today. The secretary this morning talked about 80 percent of the homegrown plots inside the United States were thwarted by local officials and citizens. That flow of information up to the feds is based on a sense of trust that the information will be handled appropriately, that individuals will be dealt with fairly; that system to preserve civil liberties is an essential part of that national security structure. The relationship with communities that are going to detect problems can only be maintained if we preserve civil liberties.

And I know that this is what the Framers had in mind because this was a group who put together this system to preserve civil liberties and a system of checks and balances – not a fuzzy-headed liberals, but a very hard-nosed pragmatic individuals who had just fought a war, who knew that perilous times were ahead, who were choosing a system they thought would be best guaranteed to preserve this very fragile nation.

MS. MESERVE: Chief Lanier? Seems like a perfect place for you to jump in.

CATHY LANIER: Well, you know, it's – a lot of questions have come up about local law enforcement's integration into this information-sharing environment and how they – well – factor in the civil liberties, civil rights and privacy issues.

But the reality is, is that that's integrated into our everyday operations. We deal with the most critical balances of civil liberties and privacy and civil rights every day. Think about my average day pre-9/11: We deal with gang violence, identifying gang members, validating gang members, striking that balance between intelligence gathering, criminal predicate to store information and use information in a criminal prosecution; everything from, you know, dealing with large protests that come to this city and doing threat assessments that may be posed because of those large protests, all of those things are deeply rooted in making sure we have good privacy policies, we have good management of those policies, and that there's oversight for those things.

The critical thing here is that the stakes are much higher. I mean, that's the difference. I think we have a real good understanding of making sure we have that transparency, the community outreach having the connection to our community, and that they trust that law enforcement is a legitimate partner in this – in this fight.

So what's most important for us now going forward into this information-sharing environment post-9/11 is that we don't lose that legitimacy. We have to remain transparent; we

have to be part of this fight, I think, even more so in the past few years as the internal threat inside of the United States has grown.

So we take that very seriously. And I think as partners in this integration going forward with the information-sharing environment, we have to really make that our priority, because when we lose that legitimacy – I mean, think about it; after all, our source of information, our best defense is the community. If we alienate those sources, we lose the ability to detect, deter and prevent.

So we deal with that every day. That's how we close homicides; that's how we stop gang violence. So we value that relationship, and we just have to make sure that that stays a priority going forward.

MS. MESERVE: Administrator Pistole, if anybody's been in the hot seat on this whole issue of privacy and civil liberties, it's you, so –

CHIEF LANIER: And we've enjoyed watching – (inaudible). (Laughter.)

JOHN PISTOLE: Yes, I think –

MS. MESERVE: It's so hot that he's moving around.

MR. PISTOLE: I was trying to help out there.

MS. MESERVE: So give us your thoughts.

MR. PISTOLE: Well, obviously, being the head of TSA gives a person the opportunity to hear a lot of different opinions –

MS. MESERVE: (Laughs.) All the time.

MR. PISTOLE: – on the proper balance between security and privacy. And obviously, with the creation of TSA in November of '01, two months after 9/11, the focus has been and will continue to be on the best possible, most effective security provided in the most efficient way, recognizing that we have to and strive to, every time that we encounter a passenger, 1.8 million-plus times a day, that we respect the privacy and civil liberties of each of those passengers.

Now, the challenge is that each person in this room and watching has perhaps a slightly different definition of what that proper balance is. So, for you, something may be completely appropriate and necessary for security, and for somebody traveling with you, they may say, that's way too far, I don't want to go through one of those machines, I don't want to be patted down.

And so how do we give the highest level of confidence to the traveling public on every air flight, every flight, 17,000-plus flights a day in the U.S., over 50 million people a month – you know, just big, big numbers. You think of a business that encounters that many people, in

customer satisfaction surveys, to be in the high 90 percent is significant. So based on things that we deal with, we try to ensure that we are doing everything we can.

There's two things I would highlight that we are doing, have done or will be doing that highlight the privacy/civil liberties aspects: One is our conversion of the advanced imaging technology machines to the automatic target recognition, which just gives a generic outline of a person. And the passengers are able to see that right there; some of you have been through that and see that – identifies an anomaly for resolution. I'm pleased to announce today the – our acquisition of 300 more of those machines, and so those will be deployed – airports that you travel through in the – in the next several months, and so that will increase the number of those machines and give us that best possible security against the nonmetallic type device – the bomb that was on Christmas Day '09 – with the highest level of privacy possible – that's one.

The other issue that we're dealing with is part of our risk-based security initiative where we're trying to get away from the one-size-fits-all construct and recognizing that, as we can get information from people on a voluntary basis, that we can then perhaps provide a different level of physical screening because we know more from an intelligence perspective. So intelligence is driving what we're doing on the front end so we can do the physical screening perhaps in an expedited way.

Again, that's all voluntary. If people want to share information with us, at this first iteration it will be through frequent flyer elite programs, and certain airports will be rolling that out next month in four airports. And so we have the opportunity to do some things that recognize we can provide the best possible security in the most efficient way, recognizing the privacy and civil liberties of all passengers.

MS. MESERVE: Let me follow up on the imaging machines which have been so controversial.

MR. PISTOLE: I thought you might.

MS. MESERVE: Yes, well – (laughter) –

CHIEF LANIER (?): I was hoping you would.

MS. MESERVE (?): We've been through this before. (Laughter.)

MR. PISTOLE: OK. Just show of hands. Have you been though an advanced imaging technology machine? OK. OK. OK.

MS. MESERVE: I want to see the show of hands if you refuse to go through a body-imaging machine.

Am I alone? Two of us?

MR. PISTOLE (?): Yeah, OK.

MS. MESERVE: My question has to do with the fact that you've changed the machines now. You've changed this software. So you're not showing the anatomical detail. Is that an admission that TSA got it wrong?

MR. PISTOLE: I think it's a recognition that we could do better. So the first – the technology – no, just being very frank that the technology that was in place had all the privacy protections for that type of technology that could be in place. So a separate room with an image operator seen the image, never saw the passenger; the security officer saw the passenger, never saw the image. So – and the machines had – did not have the capability to store or transmit the images.

So, as good a privacy protections could be built in for that technology were in place; this is the next generation, if you will, that gets away from that outline of a specific person to that, simply, of a generic outline of person, which, again, in complete transparency, the passenger can see right there and they can say, oh, yeah, I forget that I left a card in my pocket or whatever it may be.

MS. MESERVE: I'll let you off the hook for now.

Suzanne, I wanted to follow up on something you said about, this isn't a zero-sum game, that you can have both privacy and security at the time.

But in the last couple of days, a couple of developments: An appeals court ruled against the Justice Department when it came to tracking individuals with cell phones. And, also, you had an AP poll that came out showing that a majority of Americans, if they had to choose between security and civil liberties, a small majority would choose not to give up their civil liberties.

What I'm wondering is, if, 10 years after 9/11, we're seeing something of a backlash, something of a rethinking of this issue. And does that pose security challenges, or is that something we can and should embrace?

MS. SPAULDING: Well, it's interesting. I think it is – I think it does reflect that the ground is starting to shift beneath our feet. And I will say that it worries me, as somebody who has spent many years in the intelligence community, both at CIA and then in the oversight and on various commissions, for my colleagues in the national security world who are out there running full steam ahead under a – under a certain understanding about what America is asking of them. And I've seen this happen before. And they don't quite realize that the ground is starting to shift, and when something goes wrong, what the reaction will be back home where the level of fear has been reduced, where we are – we are hoping to move to a place where we can put terrorism in a different kind of perspective.

So I think the court's decision on geolocation – which was saying, you know, a long-term watching every single place someone goes is different than simply either following them or putting a tracking device on them for a day; it's the difference between a day in a life and the

daily life of a person. And I think it has implications for the way that government currently accesses third-party records and the understandings there about – with regard to privacy interests where, I think, a difference in quantity is becoming a difference in kind.

MS. MESERVE: Matt Olsen, let me ask you: Stewart Baker, a former official with the Department of Homeland Security, argues that privacy campaigners have actually undercut security. Do you agree with that?

MR. OLSEN: Well, I know Stewart; Stewart preceded me at some point as a general counsel at NSA.

No, I think that – along with what Suzanne said – that we need to see that privacy interests – and I think this is the same thing that you said, Chief – you know, that being transparent and adhering strictly to the letter and spirit of the Constitution and the laws that govern our activities actually builds confidence in what we're doing. It allows the people who provide this information, whether that's people on the street, other agencies, to be confident that that information is going to be handled appropriately.

So I actually think that that's – that that commitment is a strength and actually has the potential – and does, in fact, bolster national security.

I think the trick and the challenge, at times, is to – again, I think this is – along with what you're saying, Suzanne – is to know where the lines are. And the challenge in the intelligence community is to – those lines are sometimes blurry and the laws change and views shift. And what I see is what Suzanne identified, that it's very important for operators to have clear rules. And when we have clear rules we follow those rules.

MS. MESERVE: But you're operating in a clandestine environment. So how do you reassure the American public that those rules are in place and those rules are being observed?

MR. OLSEN: That's a great question. You know, it's – much of what we do is secret by design, and needs to be secret. And so there we have institutions and processes in place to ensure that those rules are being followed and to give the American people the confidence and trust they must have in their intelligence community. And that's typically and primarily Congress and the congressional oversight committees. They do that job and they do that job quite well.

But in addition to that there is – you know, within the executive branch, I can speak to the role that the Department of Justice plays in providing that kind of oversight of the intelligence community. So I think there's actually strong and vigorous oversight, although not the same because, again – as another context, because of the secret nature of much of what happens in the intelligence community.

MS. MESERVE: You know, General Hayden set the table for this discussion beautifully and talked a little bit about the domestic threat requiring this integration of information from the federal down to the local level. And he said that there were boundaries that are part of our DNA.

Chief Lanier, I wonder if you could talk a little bit about that; about whether it is, in fact, harder perhaps to integrate all this information and intelligence from the federal to the local and back up again because of those boundaries. What kind of impediments are there to true information sharing?

CHIEF LANIER: Well, first there's two different – I was listening to Matt talk, and there's two different types of privacy and civil rights issues that we have to deal with now post-9/11, and to a certain extent before 9/11. The first is the physical security. That's the, you know, setting up the machine that's going to make everybody go nuts trying to screen people going through the airport. You can do some things to lessen that by doing outreach and bringing in a small group of civil libertarians, have them – you know, demonstrate the machine up front, get their feedback up front before you launch it. So you can get input on physical security.

After the WTO riots in 1999, we had our first big World Bank conference here; we went from security fencing that was bike rack to concrete jersey barriers and, you know. But we had to go in and do outreach to the community. And we met with, you know, parking lot attendants and owners and we got them to agree to security measures, so it went smoothly. And we did checkpoints and searches and all that that normally would not go over very well. But because we had time to bring the community in and get their input, it worked well.

With intelligence it's very different. It's so much harder to go out and get that buy-in – it's impossible to go out and get that by-in from the community. But now my job at the local level is to get that buy-in from the community because I have See Something, Say Something. I've got – I'm launching a major iWatch program today when I leave here. So I have to have some way to bring the community in to get that information and assure them that what is pushed up into the federal shared space of the intelligence community is something that doesn't infringe upon their rights. So in other words, I'm not an agent for the CIA. (Chuckles.)

MS. MESERVE: Well, let's talk about the New York Police Department then.

CHIEF LANIER: Which I figured you would. (Laughter.)

MS. MESERVE: As you may know, the Associated Press has recently reported that there is a very close relationship between the CIA and the NYPD and that the CIA is training some NYPD personnel, that there are CIA personnel at NYPD headquarters. And it's raised a lot of questions about the balance between spying and policing. Is this problematic for someone like yourself? You say you want to build a close relationship with the community, but if a police organization has a component that is going into a community and operating covertly – going even into mosques, according to this AP report – does that exactly undermine what you're trying to do?

CHIEF LANIER: Well, I'm going to stay away from commenting specifically on NYPD, because – (chuckles) – that's just the smart thing to do. (Laughter.) But I will say that, you know, we've always operated on a principle that there – intelligence is a process that is – we get tip information or source information, we begin to investigate that, and if we develop a criminal predicate, then the investigation kind of moves on. In this case, what we're asking of

the community is to report to us behaviors – not profiles, not personal identifying information to a certain extent – we're asking them to identify behaviors, report those to us.

And if there is no connection to terrorism, there's no connection to a criminal activity, all that personal information is stripped away. It's not stored anywhere. We're not keeping dossiers; we don't have a database. I think that's the right way to go about doing it because the information that you're going to get is going to come from somebody who goes to the mosque. And we've had cases like this, where regular participants that go to a religious – whether it be a mosque or a Catholic church or whatever – saying, you know, there's a person that's –behavior's very suspicious and we think you should look into it.

And then it's perfectly appropriate to determine whether there's a criminal predicate or there's a terrorism connection, and if so, then to move forward. But there has to be that initial analysis, there has to be that initial vetting and then pushing that information up, if it's counterterrorism-related, pushing that up to our federal partners and handling that the right way. That's how you keep people's trust. That's how you keep people reporting suspicious activity. And that's how you do it without violating people's rights.

MS. MESERVE: Suzanne, you're the one non-governmental person up here – your thoughts on that program as reported by the AP and its implications?

MS. SPAULDING: Yeah, well – and it's hard to know what the facts are here. The article itself pointed out that there was some pushback on their portrayal of the facts so, like Cathy, I'm going to be careful about assuming the facts, you know, that have been put out there.

But I do think – you know, we heard this morning how important it is to have that seamless relationship. Clearly some of the training, it seems to me, is not inappropriate. The thing that raised, you know, real red flags in my mind was the assertion that there was somebody still on the CIA payroll who was sitting in Dave Cohen's office as his deputy.

I think that's, you know, clearly very troubling in light of the restrictions that we appropriately put on CIA with regard to intelligence collection in this country. And the assertion that they were – that – the other thing that I thought was very troubling was that the city council was not aware of a lot of the activities that are going on in NYPD. I do think that the issue of local oversight – I think it's raised particularly by the JTTFs, but apparently it's also raised by some of the activities of NYPD – making sure that you've got that local oversight by the mayor, by the sheriff, by the city council is critically important.

MS. MESERVE: Let me segue to a little discussion of fusion centers, which have proliferated around the country. And they're engaged in some of this gathering and collating and distribution of information. DHS has now tied privacy policies to funding in an effort to address this very issue that we're discussing today. But is there inconsistency amongst the fusion centers? Matt, also maybe you can tackle that.

MR. OLSEN: I'm tempted to hand it over to my colleague here from DHS. (Laughter.) So I really don't – you know, I really don't have a lot –

MR. PISTOLE: TSA.

MS. MESERVE: TSA. (Chuckles.)

MR. OLSEN: Or – right, I know.

MS. MESERVE: (Inaudible) – on the job – (inaudible) – yeah.

MR. OLSEN: Yeah, I really don't have a lot of experience with the – with the fusion centers.

CHIEF LANIER: I can speak to it some because I've been engaged in – from the beginning, from 2001, the development of what later became the fusion centers. And I think it was a very good move to ensure that fusion centers do have privacy policy across the board. And there is pretty consistent guidelines in the code of federal regulations for what your privacy policies and what guidelines you should operate in. Are there still gaps in that and should there be one single kind of consistent privacy policy across all fusion centers? Yeah, probably so.

There's been some mistakes made by fusion centers. I mean, I run a fusion center, you know, in Washington, D.C. And I can tell you that the evolution that's gone through for fusion centers – you know, in the last six or seven years they've come a really, really long way. And there has been some mistakes and there will be mistakes. But I think, you know, you're damned if you do and you're damned if you don't. And you'd better be damned for doing in this world. (Chuckles.)

MS. MESERVE: And the kind of mistakes you're talking about?

CHIEF LANIER: I'm sorry?

MS. MESERVE: And the kind of mistakes you're talking about?

CHIEF LANIER: The ones that I've seen have been information that was passed on from agency to another, third-party information, that wasn't approved to be shared or probably wasn't appropriately shared with personal identifying information; some information I've seen with regard to protest activity and political affiliations, you know? Those are evolutions that local law enforcement should – most of the major cities have been through years and years ago. But some of the newer fusion centers coming online that are not in a major metropolitan area and haven't been through that evolution – that's a learning curve for them.

So I think the consistent privacy policy and the, you know, across-the-board implementation of the code of federal regulations for them – all those things are going to be important. But we can't throw the baby out with the bathwater; there's going to be mistakes, there's been mistakes. But I think the fusion centers are an important part of this network that we have to form for homeland security going forward.

So, you know, we just have to be tolerant and put the effort in. As in the paper that was released today says, we have to put the effort in. If there's a – if there's a training issue, let's address it. If there's a policy issue, let's address it. But let's not throw out something that's eight years in the making that's finally starting to add value.

MS. MESERVE: You suggested that there are improvements that can be made. Have you got any specific ideas on how to bring better consistency amongst the centers and make the system work with more attention to privacy and civil liberties?

CHIEF LANIER: Yeah, I think the – I think there needs to be kind of a single effort – a singular effort across the board from the federal agencies because, again, this is – if you're not in a major metropolitan area, you're not in a major city, a lot of those privacy issues are not something you deal with every single day. It's a different type of privacy issue – the stakes are much higher here.

So I think that the intelligence community and the federal agencies have to take that on to educate the – these fusion centers and make it consistent across the board because where it may be well understood in one major city, it may not be well understood in a state agency that has a lot of rural participants in there. So I just think that that has to come out as a consistent policy, consistent training across the board, from those who know it, who've been doing it for many, many years.

MS. MESERVE: Something else for you to worry about.

MR. OLSEN: Exactly. Yeah.

MS. MESERVE: You know, NCTC does this on a much grander scale, of course, combing through the databases and collecting the data. And it does give some people the heebie-jeebies to think that there's a big brother, all-seeing eye up there gathering this data from all kinds of sources. Is there anything you can say to reassure people that you're staying in the right lane and you're not just conducting a dragnet?

MR. OLSEN: Sure. I mean, first of all, NCTC is not a collector in the same way that other intelligence agencies are collectors of information.

MS. MESERVE: You're an integrator.

MR. OLSEN: We're essentially an integrator. We obtain information from other agencies – other intelligence agencies and law enforcement agencies. I mean, really, NCTC was an outgrowth of one of the key insights post-9/11 that we've all touched on. And that is that there really shouldn't be this distinction between law enforcement and intelligence. It doesn't really make sense to – information; doesn't really make sense to make that distinction. And it doesn't make as much sense –

MS. MESERVE: Well, aren't there – aren't there boundaries? Shouldn't there be boundaries somewhat between law enforcement and intelligence?

MR. OLSEN: Well, when it comes to terrorism I think the answer is no. I think it – when it comes to counterterrorism that information that relates to an act of terrorism in the United States is no different from intelligence about that – about that act or about that threat. And we need to be able to put that information together. I mean, that was one of the key, you know, changes to the law post-9/11; that was to take down the wall that existed between intelligence information and law enforcement information that prevented FBI agents from talking to each other – one on the national security side and one on the law enforcement side. So we really, I think, at NCTC are the sort of embodiment of that recognition.

The other aspect is the sort of distinction between foreign and domestic. Certainly there are laws that apply to certain types of collection activities when they occur in the United States versus outside the United States. But when those laws are followed and then we get that information, the key that – I think the contribution NCTC makes is the ability to look at all that information in one place – domestic and foreign. But the information we get has been lawfully collected by others. We integrate it and then analyze it and then share it.

MS. MESERVE: Civil libertarians have raised the question of redress. If you have information about someone and it's simply not correct, what can they do about it?

MR. OLSEN: Well, there's a process for – and particularly with respect to watch-listing – for redressing if there's a mistake, if someone is wrongly placed on the watch list. And that happens – that is effectively – you know, that's successful hundreds of times a year.

MS. MESERVE: Profiling – one of those words that comes up a lot when we discuss privacy and civil liberties. And Administration Pistole, on that score –

MR. PISTOLE: I know NCTC doesn't profile. (Laughter.) I know the chief doesn't profile. I know Suzanne does not.

MS. MESERVE: But does the TSA? Here's the question.

MR. PISTOLE: The TSA does not profile. So – yeah, obviously there's been a lot of talk about –

MS. MESERVE: But the behavior detection officers.

MR. PISTOLE: OK, sure.

MS. MESERVE: Let's talk about it in regards to that.

MR. PISTOLE: Yeah, so the question about how can we use intelligence in a more informed fashion to make judgments about each individual looking at the person rather than the prohibited items that that person may carry – that's one of the ways we wanted to go an organization in trying to be a risk-based, intelligence-driven organization. That being said, we have to make sure that we don't profile – that we use information about the person that they

either share voluntarily through this known, trusted travel program that we're working on with airlines and airports who would provide a dedicated lane – that's all voluntary. So if somebody doesn't want to share that information, that's fine, they would go through the normal screening process.

For those other issues – for example, we have a number of behavior detection officers; and you've probably read about what we're doing at Boston Logan Airport – some of you have been through there, perhaps had a brief conversation, engagement with the behavior detection officer and assessor. The whole purpose is to try to get away from the one-size-fits-all to use what some people describe as an Israeli model – that's a – that's a very broad brush – but to use more information about a person.

Are they exhibiting any suspicious activity? Any cop, any law enforcement officer can tell you in just a few seconds, really, of talking to somebody, is there something up about that person. So the whole idea is to take that information and use it in an informed way and to, if feasible, to expedite that person's screening or to – do we need some follow-up questions? So that's the whole premise behind it. As we move forward with that if – we'll see, do we need to recalibrate, do we need to make sure –

CHIEF LANIER: You know, I got to jump in on the profiling –

MR. PISTOLE: Jump.

CHIEF LANIER: – for just a second because, you know, profiling became a dirty word because of issues in local law enforcement. So I – but I have to say that it's not necessarily a negative thing if profiling is looked at appropriately and done the right way. The drug courier profile on mass transit for many, many years was very successful. You know, person pays cash for a one-way ticket, no luggage – it just – it identifies something that is an anomaly that was consistent with drug courier profiles. It didn't make reference to race or, you know, any of the things that are associated with negative profiling.

So I think you – again, you can't throw out the baby with the bathwater here. There are some positive ways to profile behaviors, to profile other things other than physical characteristics that can help you decide if there's a more intensive look that needs to be taken. So I think just the whole concept of profiling all being negative is a bad way to look at it.

MS. MESERVE: We're getting some great questions in from the audience. There are cards; if you've got questions, send them in. I'm going to start using some of these because they're good.

Chief Lanier, one of these is a follow-up to something you said about discarding information if you don't find a link – you don't find anything detrimental. This questioner asks: Don't you run the risk of later finding it was one of several warning indicators? In other words, could there be a case where several early indicators might really prove to be valid later? Should we retain the data? Should it be shared?

CHIEF LANIER: Well, the rules that the – the rules are pretty complicated, but if you're retaining anything it has to be separated – it has to be kept separately; it's not accessed; it's not shared. I think it all depends on what the – if it's suspicious activity reporting, behavior information – we do this all the time now, and this is a current battle that I'm facing with hate crimes reporting – tracking hate incidents versus hate crimes – there's a real demand for me to document incidents where people are, say, verbally harassed with hate speech. Hate speech is not a crime. I mean, look at Von Brunn. The FBI took a beating on Von Brunn because he was a known hatemonger but he had never crossed the line to anything criminal. So you really don't take any action. So we have to meet that balance again.

So my balance is for me to track those incidents without tracking identifying information, because no crime has been committed, and then using that as an analytical tool more so than an investigative tool. And that's the balance that we have to strike. So that information is retained in that sense, but if we keep anything identifying at all it is separate from anything else and it still has to be purged if there's no criminal predicate associated.

MS. SPAULDING: And Jeanne, I'm sorry, but I do think that when we talk about data retention – because I've heard this argument for years, that you shouldn't throw away any information you ever – you ever got because someday it might be relevant to something. And I think it is a reflection of a – of a larger problem in this whole arena, which is this chasing the myth of risk elimination rather than acknowledging that what we're engaged in is an exercise in risk management.

So it's both recognizing that there are national security costs to privacy incursions – so there's some costs there to keeping that data, not to mention the potential risk of a cyber incident and that information becoming public, and recognizing that every little thing that you – you know, that you – that you might want to do is – does not mean that you should pursue that – and that, in fact, when you chase that myth of risk elimination you're ignoring risks that you're creating by doing that in other places.

And retaining everything may make you feel you've eliminated the risk that you won't have that information when you need it, but you've created a risk of public backlash and of exposure.

MR. PISTOLE: And I'm glad Suzanne mentioned that because that's the whole approach that we in TSA are taking in terms of ensuring that we are doing the best possible job to mitigate, to manage risk, but not to eliminate risk. If we truly want to eliminate risk, we would have at least two hour lines in every airport; worldwide global supply chain cargo would be shut done for weeks at a time. So the whole –

MS. SPAULDING: And you still wouldn't have eliminated –

MR. PISTOLE: And we still wouldn't have that. So the reality is that we are in the risk-mitigation, risk-management business with the traveling public, with the airlines, with everybody in the mass transit area.

MS. MESERVE: You mentioned cyber. Let me turn a corner there, if I could. The systems in which you store all this information, how safe are they? Every day we read about another incursion into a government database by a foreign entity.

MR. OLSEN: Well, you know, I think there's reason to be concerned about the security of all this information from a cyber perspective. I don't think – you can hardly pick up the newspaper and not read about some sort of cyber intrusion whether at a government agency or a company. So I think there is real reason to be concerned, and I know that there's lots of effort being put into ways to try to protect that information.

And if I could just actually go back to a point on the retention because I just – as I think about – retention is an issue and it's a balance, as I think we've all tried to make that point, how long you keep this data. But retention is only one part of a broader set of controls that you can place on information in order to protect privacy and civil liberties. And it's a – it's sort of an end-to-end sort of set of procedures and systems.

So you control access; you control who can access the information; you make sure they have training. You make sure that if they do access that information, you can audit it. Then you control how long you retain it. But you also control how you disseminate it, who you can disseminate it to. So retention – I just want to make a point in that I've seen this at NCTC; it's certainly true at other places I've worked – NSA in particular – very, very strict controls from beginning to end on how data's handled.

MS. MESERVE: Security isn't the only challenge posed by cyber. And General Hayden said a short time ago that he didn't believe we had any reasonable sense of privacy really is in cyberspace. How do we grapple with that one? Who wants to jump into that? Tough one – Suzanne?

MS. SPAULDING: Well, I do think our concept of privacy is evolving. And so it is hard to figure out where those tripwires are. I disagree with those who say that young people today have no sense of privacy. Certainly we've seen there are tripwires, and when Google or Yahoo, you know, steps over the line, the community rises with one voice and beats them back very effectively.

So there is this sense of wanting to control your information, even if that doesn't mean that you're trying to keep it secret. I think it's a growing recognition on some level that keeping secrets in today's world is a losing proposition, but perhaps trying to control what others can do with your information is the next stage.

MS. MESERVE: And what about the question of surveillance and how much –

CHIEF LANIER: I was just going to say technology's the next issue. The technology that's available now is going to take, you know, a hundred years of law enforcement case law back to task, I think, because of just the availability of technology to better protect the community – having the ability to quickly locate someone through a cell phone tracking; having the – who's committed a homicide and has a victim's cell phone; having the license plate reader

system; having automated speed enforcement, digital cameras. I mean, there's a whole world of – I think that we're going to see – I mean, the cell phone is just the first one. There's a whole world of issues that are going to have to be redefined legally because of technology.

MR. OLSEN: In a general way, I just think we have to accept the idea that things are changing very fast; and it will always be the case, I believe, that the law is going to lag behind technology and our adversaries. So we see that in a number of contexts. The adversary is changing faster than the law, and technology is changing. So the law is going to tend to lag behind.

MS. MESERVE: And law enforcement has asked for some new capabilities. They'd like to be able to tap in to Internet communications. Polling indicates that that's one place where Americans are uncomfortable, when we're talking about emails between two American citizens. Who draws the limits? How do we draw the limits? Is that just done legislatively? Is this something that's going to be a long-out litigation in the courts?

MR. OLSEN: No, well the law's pretty well settled and pretty clear on how to obtain a warrant to listen in to someone's conversations or read their emails, so – on the law enforcement side.

MS. MESERVE: On telephone communications, but doesn't the technology of the Internet pose a different scenario?

MR. OLSEN: I think the law actually applies pretty well in that setting as well.

MS. MESERVE: OK.

CHIEF LANIER: Well, really the community is who sets the standard – I'll tell you that right now – because the community will drive what happens with the law. They're the ones that'll set the standard. If what currently is being done is not acceptable to the community, they will fight to have that moderated somehow. And right now I think that balance is – the community wants us to keep them safe, at the same time keep their privacy. And that balance is where we end up with the laws that we have now.

MS. MESERVE: Suzanne.

MS. SPAULDING: Well, I think that the law is pretty clear with regard to real-time communication.

CHIEF LANIER: Right.

MS. SPAULDING: It's a little less clear with regard to stored emails, for example, and it's even less clear with regard to all kinds of online activities. And so I think there is some room for going back and looking at those laws, and the community can only drive that process to the extent that the community is informed –

CHIEF LANIER: (Inaudible.) Right. (Chuckles.)

MS. SPAULDING: – and transparency is a real challenge and incredibly important here.

MS. MESERVE: One of our audience members asks, if potential illegal activities are discovered through social media sites, such as Facebook or Twitter, is this an invasion of privacy? Not being a lawyer, I'll punt it to you guys.

MR. OLSEN: So John's a lawyer. (Laughter.)

MR. PISTOLE: Yeah, I got out of that business about 30 years ago. So, yeah.

MR. OLSEN: Well, it really is very context-dependent. It's a hard question to answer, and it does depend on – very much on –

MS. MESERVE: That's why this is such a hard issue – (inaudible) – so slippery.

MR. OLSEN: Yeah, right – that it's a hard issue, I mean – but some things are public on the Internet and can be reviewed with very little predicate –

CHIEF LANIER (?): But so – so –

MR. OLSEN: – and some things require more.

CHIEF LANIER: – what matters there is, is – like for Facebook and MySpace and all of those other things, and YouTube for that matter. If it's put into a public domain –

MR. PISTOLE (?): Yeah.

CHIEF LANIER: – without any privacy restrictions or security restrictions set by the posters –

MR. PISTOLE (?): Yeah.

CHIEF LANIER: – so, in other words, on my Facebook page, if I post something that anybody who goes to my Facebook page can see, it's like on the public street, correct? And so, if I then have security measures in place, so that some of the things I post are just for people that are friends in my network, and then the government intrudes beyond that, then you start to cross that line. But I think there's a – there's an element of what is the expectation of privacy in the social media for what is posted publicly and what is posted behind security measures that we break through. (Chuckles.) That's what counts.

MS. SPAULDING: And there – and there's also – at least there used to be, when I was in the intelligence community – the issue of undisclosed participation. So if you're participating in what is a, you know, relatively public conversation where you don't have to reveal who you are or what your affinity is, that's one thing.

CHIEF LANIER: (Like ?) undercover officers.

MS. SPAULDING: But if you're then pretending to be someone other than somebody from CIA, that presents a different issue.

MS. MESERVE: Another audience member has posed a question here. They posed it, I think, better than I did. It had to do with that quote about – from General Hayden about the reasonable expectation of privacy and what constitutes that on the Internet. This audience member asked, what specific challenges does technology and easy government access to so much electronic data pose to American civil liberties, and how should we address it?

MS. SPAULDING: So, you know –

MS. MESERVE (?): Speechless!

MS. SPAULDING: And I'll take – I'll take a little bit of a stab at it because I think it is a big and complex question.

But I do think that creating a sense that the government is out there watching and listening in a very broad way really does – again goes back to my point of undermining our national security to the extent that it breaks down a sense of trust, that it chills conversations and activity that is perfectly legitimate, because I think we derive a great deal of our strength from that marketplace of ideas from – you know, there are real national security costs to chilling legitimate activity. So I think there are some national security consequences to the government's ability, through the use of technology, to – for each and every one of us, to know intimate details of our day-to-day lives, from moment to moment, because of technology and the ability to access records, surveillance, et cetera. And I think we need to think about that.

MR. PISTOLE: Let's just make sure we're all working from the same framework though, in terms – and Matt alluded to it earlier – in terms of, for the government, whether it's the FBI on the domestic side in a criminal investigation or through the foreign intelligence surveillance court on the intelligence – the counterterrorism side. Obviously you have to have probable cause that the communicants are talking about something that is violative of a federal law, whether it's counterterrorism or criminal, and that probable cause has to be proven to either the district court judge, federal district court judge or the FISA court judge, and that judge has to approve that. And so there is a rigorous review of that whole process before the government intercepts communications, whether phone, email, whatever it may be. It's those other areas where you're talking about – yeah, what is the expectation of privacy on a Facebook post if it's – if it's something that you want just your friends to see or otherwise. So that's where there's questions.

Everybody – and there's maybe some in this – in the audience, who monitor – let's say – jihadist websites on their own and then may report that to MPD or the FBI or CIA. And so if that person's not acting as an agent of the government, then the question becomes, can that be

used and how so? So, there are rigorous protocols and rules in place; so it's not just like the government's out there doing all these things.

MS. SPAULDING: But we don't have rules really – we – the ground – we haven't yet figured out the geolocation, for example, across the spectrum from the, you know, after an incident, all the way through to putting something on somebody's car for a week or two weeks or a month. And so I think there are areas where we haven't yet quite figured out what the – where the lines are.

MR. OLSEN: But in some ways, I do think that makes the point, that there are some areas that are gray areas that are evolving. In that case – in – there was a D.C. case involving the

MR. OLSEN: – geolocation. And I was a prosecutor in D.C. for many years, working with the Metropolitan Police Department, and there was the general view that a tracking device on a car, over a short period of time, didn't require probable cause.

CHIEF LANIER: Right.

MR. OLSEN: Now, you know – so now we're in a new area that – and the D.C. circuit is – has issued this opinion.

But the point, I think, that John makes is a really important one, and that is that this idea of sort of widespread government surveillance, outside of the rubric of judicial and congressional oversight, is not an accurate picture at all.

When it comes to surveillance of phone conversations involving U.S. persons, that's done with orders given – provided by the FISA court based on a very rigorous review procedure. And at the – and what must be established is the same standard that's required to – for someone in the Metropolitan Police Department to get a search warrant, and that's probable cause. So it's a very, very rigorous process to get the kind of approval that's needed to conduct the sort of surveillance of communications that that question raised.

CHIEF LANIER: You know, and even in that case – a lot of people don't realize that – even in that case, through abundance of caution, the detectives got a warrant. It was the timeline that was the issue.

CHIEF LANIER: They actually without – I mean, they went and had a judicial review and got a warrant for the tracking. It was the timeline and how long the tracking – when it was placed and how long it was on there was the issue. So, you know, just to clarify that a little bit.

MS. MESERVE: Another question from the audience, and this one, I think, Mr. Olsen, goes to you: How do we strike the balance between identity data requirements to facilitate effective identification of terrorists and being inundated with data? Not exactly a privacy question.

MR. OLSEN: Right, I mean, the issue –

MR. OLSEN: – one of the things that we're doing, and I think this is – we've tried to step this up at NCTC following the failed attack of this December 25th, 2009, in Detroit – is to really enhance our watch-listing information. So the information that we already have on identities, we've really tried to make an effort to go out and find other sources of data, to get as accurate a picture as possible of the identities of the known and suspected terrorists that are then placed on watch lists. I mean, the – I think the question might be asking a little bit about how do we deal with the inundation of data? I mean –

CHIEF LANIER (?): Yeah.

MR. OLSEN: – there, technology can help – you know, better ways to sort through data, to make sure that we're separating the wheat from the chaff. I mean, that is – I think there are improvements in analytical tools that give us more capabilities in that regard.

MS. MESERVE: Let me switch from high tech to low tech for a minute.

Chief Lanier, you mentioned See Something, Say Something. This is a campaign that's been embraced and promulgated by the Department of Homeland Security, encouraging citizens, if they see something they think is suspicious, to report it to authorities. Civil libertarians feel the hair going up on the back of their neck over that one and are afraid, for instance, that, you know, an angry boyfriend's going to report that you're doing something nefarious to the local authorities – (inaudible) –

CHIEF LANIER: But you know, that can happen today anyway. That –

MS. MESERVE: Pardon me?

CHIEF LANIER: That has always been – people could always do that. I mean, poison pens or something that have gone on – you know, people writing in stuff to law enforcement about other people in the community has always happened, and that's not changed by the See Something, Say Something.

I think the – and part of what we're doing with our launch of iWATCH today gets to what Matt was just talking about – is that you're talking about a flood of information. People will report, through those tools, suspicious behaviors or suspicious activity. We have two ways of analyzing that initially when it comes in. And first of all, you've just added 850,000 local law enforcement to the picture when you add the See Something, Say Something campaign.

So initial information can come in. It is looked at through an analytical tool, TrapWire, and it's also looked at by an analyst. And then there's a decision made as to whether this is criminal, counterterrorism, or it's useless, it's bad information – you know, preliminary investigation that it's not either of those things. But it also gives us the ability to push those legitimate suspicious behaviors up into a shared space where we can look around the country, through the network of fusion centers, if there is an increase in suspicious activity or suspicious packages around critical infrastructure. So I think the fear that See Something, Say Something is

encouraging neighbors to spy on neighbors is something that people could use as a fear long before See Something, Say Something.

So – and I tell you, you know, I implemented several things to fight crime in the city and, much to the opposition of many of the prosecutors, you know, anonymous tip lines. I have anonymous tip lines and anonymous text messaging lines. And our standards are very high, once we get that anonymous information in, as to how we vet, verify and investigate that anonymous information. But, as long as you have good policies and good management and good supervision, you can do that the right way. That's been very, very successful for us. So I think that's really going to be the key, is making sure that these things are managed the right way and they are focused specifically on behaviors.

MS. MESERVE: This is – we're coming up on the 10th anniversary of 9/11, of course, and the 9/11 commissioners recently issued a report card on what they saw as some of the successes and failures of their recommendations.

One they talked about was the Privacy and Civil Liberties Oversight Board, which is dormant. And Lee Hamilton, one of the leaders of the 9/11 commission, called that "a major disappointment." Why is it dormant? Does it reflect that privacy and civil liberties just isn't a priority?

Suzanne, do you want to take a stab at that?

MS. SPAULDING: No, I think that John Brennan addressed that. I think they've had a very hard time of, you know, filling the chair position. I – you know, it does raise a question about whether it's been high enough on the priority list –

MS. MESERVE: Has it?

MS. SPAULDING: You know, I'm not inside, so I don't know where it is on the priority list. But it seems – it's very frustrating and very disappointing that this many years into the administration, they have been unable to fill those positions. I think it's a very important role and an important body, and they need to have somebody in there who has real credibility with civil liberties folks.

MS. MESERVE: How would it make a difference, and what's happening in the interim?

MS. SPAULDING: Ideally what you would have is, then, this body of individuals that are there when the – when these policies and measures are being discussed from the outset. You know, where – there's been a lot of talk about this and it's reflected in the report – not tacking these things on at the end, but baked in. So they're there; they understand the imperatives on both sides of this issue and are there to help you formulate your policies.

And then they are in a position to be validators for you. And in this area, where we have so much secrecy, you know, it is like the oversight committees; important to have credible voices who can come out and say, I'm on the inside, I know all about this, and I'm comfortable that

we're doing this the right way. So I think it's – I think it's really important benefit for the administration, and I'm not sure everybody in the administration fully appreciates the degree to which it could be really helpful.

MR. PISTOLE: And I can give a personal example from the agency and departmental level where we have very strong civil liberties/privacy oversight as we try to move to more of a risk-based/intelligence-driven. So how do we use that intelligence, what intelligence can we use, how long do we retain data, things like that – and Mary Ellen Callahan from the department is here; Margo Schlanger also – in terms of privacy. And we've been through a recent initiative with very strong oversight in review and great feedback as to, OK, if you want to do this, here's what you need to do. And we also have a very strong privacy officer within TSA to address those issues. So at least at the department/agency level, I see that working very strongly.

MS. MESERVE: Is there a need though for harmonization across the federal government?

MR. PISTOLE: Oh, I think so – clearly. And that's the reason the commission made a recommendation to get that position filled.

MS. MESERVE: I want to take one more audience question here.

Matt Olsen, this one's for you: How do you ensure that the appropriate federal agency is involved at the local level? This person raises the reports about the CIA and the NYPD: Are they the appropriate people to be interfacing with the NYPD, or should it be the FBI? Did someone overstep, and who was it?

MR. OLSEN: Yeah, well, from NCTC's perspective, we work with FBI and DHS in our interaction with Chief Lanier and with the state and local agencies. And I mentioned before, we have an organization that helps us write things that then get downgraded and sent out to state and local police officers. I would say – so I – really from our perspective, it's the FBI and DHS.

And going back to something you said, Chief, that, you know, having been a prosecutor, you know, the level of intelligence that police officers on the street produce every day, both from information they're getting from the street, but also from the criminal justice system, that the – that the level of intelligence that's generated out of the criminal justice system is pretty phenomenal. There's almost not a murder in D.C. you couldn't go to a police officer on a beat and say, who do you think might have been involved?

CHIEF LANIER: Immediately.

MR. OLSEN: It's a long way to get from that to evidence in a criminal case; but it's very important to realize that what you're doing is intelligence on the street.

MS. MESERVE: Suzanne, well, we had a conversation before this panel began. You talked to me about the concept that the American public owns this government and, as the owners of the government, they should know what's happening inside it. I can tell you, as a

reporter, our efforts to find out what's happening inside the federal government have frequently been thwarted by – we're told that information, for instance, is SSI and can't be released. Is there over-classification, and is that hurting this transparency that we're talking about so much?

MS. SPAULDING: I don't think there's any question that there's over-classification. I don't think there's any disagreement about that. There may be some disagreement about the degree. But there's no question that we have a system that classifies by default and, as a result, we have, you know, over-classification.

I think more fundamentally we have too much classification and not enough transparency that is premised on, again, this illusion that somehow we really can keep this information secret. And given the counterintelligence challenge we face today, my worry is that we're not keeping it secret from our adversaries; we're only keeping it secret from the American public and from others who could help us and would benefit by getting that information.

Clearly one of the big challenges in the necessary cooperation with – at the state and local level and with the private sector is classification. And the answer to my mind is not giving out more clearances and bringing more and more people under that classification tent. If Dana Priest's right and we have almost 850,000 people with clearances, that's a lot of people with access to your deepest and darkest secrets potentially.

MR. OLSEN: Oh, so that's not true, though. I mean, there aren't 800,000 people with access to the deepest and darkest secrets of the American people – (inaudible).

MS. SPAULDING: So give us the real number. (Laughter.)

MR. OLSEN: Well, no, that's just – it's just an exaggeration. It's just an exaggeration to put it in those terms. It's just –

MS. SPAULDING: Yeah, I had to try.

(Cross talk.)

MS. SPAULDING: But I do think – but I do think that the point really is that we need to find ways to get that information, as was said earlier today, to be releasable rather than continuing to classify and try to get – and solve the sharing problem by giving more and more people clearances. It seems to me that's not the right way.

MR. PISTOLE: So I'm trying to stay in my TSA lane, but with almost 47 years of FBI, I just –

MS. SPAULDING: Oh, come on. Be wild. Get out – (inaudible).

MR. PISTOLE: – just the discussion. So one of – one of the key changes in the FBI post-9/11 is on the information-sharing and the whole idea of going from fairly restrictive

sharing, not necessarily based on classification, but just on need-to-know, typically, evidence for a criminal prosecution.

MS. SPAULDING: Need to know – need to know is the killer.

MR. PISTOLE: So the question became then, how can the bureau change to deal with the new reality of the integration? And it really became – and there's people in the room helped – partially responsible for that – share by rule, withhold by exception, on a need-to-know basis. So as many people as needed to know, that information was pushed out to. But the key became, did they actually need to know?

So, as to your SSI point, the question becomes an individual intel product or an SSI document, in and of itself, may not reveal any deep dark secrets. When you compile those in a way that can form a picture of, let's say, a security checkpoint capabilities – detection capabilities – well, we know that bad guys look at the TSA website, for example, look at manufacturers' websites to say, what are those detection capabilities? And can they go to school on that to come up with a new type of device that defeats those capabilities? So, yes, that is important, but that need to know is still part of that equation.

MS. MESERVE: Matt, do you want to weigh in on this?

MR. OLSEN: And I just – I agree with that. I mean, I think that there's a – there's a need to classify a lot of the information that we're talking about in terms of protecting sources and methods, and it's important to acknowledge the role that classification plays in protecting the ways that we are able to obtain information or protecting the – (inaudible) – that need to be protected.

CHIEF LANIER: I mean, it goes back to the last few terrorist attacks. Think about some of the information. You could almost surveil a target and get all the information you need to carry out an attack through, you know, the Internet – all public information. So what is it that you can withhold that's reasonable to withhold to, you know, increase security or make sure you maintain some security?

I mean, almost every exercise we do, we'll (red-cell ?) an event or a site, and we (red-cell ?) it all on the computer. It's all news clippings and public information that you can pull off of public sites. So where do you draw the line on what you can release and how that gets put out there – it can be used against you.

MR. OLSEN: So – and one of – one of the things that I think is really important that is part of this whole conversation is the effort to take intelligence information, counterterrorism information, and push it out – DHS and FBI do this – to – at an unclassified level so that state and local police officers and departments can use that information to have a better idea what to be on the lookout for.

MS. SPAULDING: And the more you can declassify, unclassify, not classify information and shrink the universe of information that you're really trying to keep secret, the

better off – the better your chance you're going to have of keeping that really sensitive information secret.

MR. OLSEN: Right, that's right.

MS. MESERVE: You said, Suzanne, early on, that this isn't a zero-sum game, that you can have both. You can't always have both, though, can you? I mean, we can't sugarcoat this and say, yes, embrace transparency in every instance?

MS. SPAULDING: And it's not – the point is not that they don't come into tension on occasion. The point is that you have to recognize the national security costs of privacy intrusions, of intrusions on civil liberties, of weakening the system of checks and balances, of –

MS. MESERVE (?): With our –

MS. SPAULDING: – of failing to have adequate transparency, that that – that that – that that they are, in and of themselves, important elements of national security. And so if you – when you have this tension, it's not national security over here and these other things over here. It is, how do we manage these risks in a way that maximizes national security? And in some cases, that's going to be maximizing the protection for civil liberties and privacy because there are national security costs to failing to do that. So it's not just, we need to do both, and it's nice to try to do both, and they never run into tension; it's recognize the national security costs of failing to deal with that.

MS. MESERVE: What are those costs? Can you be more specific?

MS. SPAULDING: So again, I think that – I think the folks who are on the front line fighting this every day have been very eloquent, particularly Chief Lanier, about the costs of undermining the trust that you absolutely must have with your communities and then between the state and local and the federal level. That – I think that's one of the, you know, very fundamental ways in which that's a national security cost.

Someone earlier, Ozzie from CSIS, made the comment earlier today about the most important thing that their study concluded was that we need to not fuel the terrorist rhetoric, the narrative that allows them to recruit; and that is that the U.S. is at war with Islam. Well, that's a – that means there are very real national security costs to the measures we might take that would perpetuate or allow terrorists to claim that this is targeting – this is profiling Muslims, that increases sense of alienation –

MS. SPAULDING: – from the rest of society, that make them feel as though they are unfairly targeted. That's not just a civil liberty value, although it is in and of itself; it is a national security imperative.

MS. MESERVE: Does the polling data that I referred to at the beginning, that people right now are more interested in preserving civil liberties than securing the country, does that indicate that we haven't got it right yet? What do you think?

MS. SPAULDING: I think it's fascinating and I would – I want to read the question. Senator Warner raised some questions about exactly what did that reflect. I think it's encouraging. My sense is, having watched these polls over the years, this is the first time that we've seen that number, I think, over 50 percent. And I actually think it's – I think it's encouraging.

MS. MESERVE: And worrisome at all to those of you on the enforcement side?

MR. OLSEN: It's not worrisome to me. I – you know, I think it's a – I think Suzanne put it well. I think we need to continue to work at this, and it's a very dynamic environment, and those polling numbers could change. I think we need to also realize that it could change pretty quickly.

MS. MESERVE: Especially if something happens.

CHIEF LANIER: – something happens, it will.

MR. OLSEN: Exactly. And so I think our – it's incumbent on us as leaders in this community to try to give guidance and direction to the people that work around us and to be as clear as possible about the rules.

Again, my experience has been at Justice, at NSA and now at NCTC, that the people on the front line want to know what the rules are; they are committed to following the rules. It's just sometimes hard in a very dynamic and fast-changing environment to know exactly what the law is on a particular time or day. And so – and when what the poll – the polls are even more fickle. So I think our responsibility is to – is to be leaders and to be – give direction and guidance and – but the bottom line is, people are trying very hard to follow those rules.

MS. MESERVE: And that sounds like the perfect place to wrap it up.

Thank you very much to Matt Olsen, John Pistole, Cathy Lanier and Suzanne Spaulding to INSA and CSIS for letting us have this discussion, and for all of you for listening and for your input with your questions. Thank you. (Applause.)

(END)