BRENNAN
CENTER
FOR JUSTICE

Brennan Center for Justice
at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646.292.8310 Fax 212.463.7308
www.brennancenter.org

Transcript

Intelligence Collection and Law Enforcement: New Roles, New Challenges

Friday March 18, 2011 | New York, New York

Panel 3 of 3
Regulation of Domestic Intelligence Gathering and Potential for Reform

Shahid Buttar
Executive Director, Bill of Rights Defense Committee

Aziz Huq
Associate Professor of Law, University of Chicago Law School

Philip Mudd
Senior Research Fellow, Counterterrorism Strategy Initiative, New America Foundation;
former Deputy Director, Federal Bureau of Investigation, National Security Branch

Suzanne Spaulding
Principal, Bingham Consulting Group;
former Assistant General Counsel, Central Intelligence Agency

*Moderated by **Emily Berman***
Counsel, Liberty and National Security Program at the Brennan Center for Justice

---

Emily Berman: Good afternoon, everyone. Thanks for staying until the bitter end and the last panel of the day. And I want to extend a special welcome to our panelists who I'll introduce briefly in just a minute. But first, I want to set the stage for the topic of this panel, which is the regulation of domestic intelligence gathering. As we've heard people reference throughout the day, there are many sources where limitations on law enforcement's power to collect intelligence might come from. So of course, there's the constitution, statutes such as the Foreign Intelligence Surveillance Act, the USA Patriot Act, and then some regulations that people are often less

familiar with, though they've gotten some airing today are the internal guidelines that agencies generate.

And of particular relevance, of course, are the Attorney General Guidelines for the FBI's domestic operations. As Fritz told us at lunch, those grew out of the Church Commission's investigation and the revelations of the intelligence community's activities then. And they actually reflected a lot of agreement between the Justice Department and Congress. Congress was heavily involved in working out what the content of those guidelines, which would be, initially, they thought they might pass a statutory charter for the FBI. Instead, they went with the internal regulations, but they did reflect a lot of input from Congress. So over time, they've been subject to a lot of revision and adjustment.

And the most recent changes were implemented in 2008 by then Attorney General Michael Mukasey. And they included significant alterations to the rules. I think the Justice Department often characterizes the changes as merely a consolidation in bringing the rules in line with one another in various contexts. And I don't see it that way. I think they extended a lot of new powers to the FBI. And among other things, the guidelines now permit, for the first time, a level of investigative activity without any factual predicate to suspect criminal wrongdoing or a threat to national security. And at that assessment stage, the FBI is authorized to use very intrusive tactics such as infiltration of mosques, constant physical surveillance, asking questions while pretending that they're not an FBI agent.

So things that used to be reserved for much later stages of investigation when there was more reason to be suspicious are now available pretty much immediately. So those changes have proven to be quite controversial. And as you've heard, it remained subject to debate. But it shouldn't be surprising that rules in this context spark controversy because, as we've heard today, the efforts to determine what the rules should be raise some really difficult questions. So for example, in the wake of 9/11, the focus of law enforcement shifted much more markedly to prevention to intercede before attacks can take place rather than the investigation and prosecution of crimes that have already happened.

John Ashcroft's guidelines in 2002 explicitly made that the primary mission of the FBI, and the Mukasey guidelines from 2008 just sort of carried that idea forward and even expanded it. But what exactly does it mean to focus on prevention in terms of an investigation? What information and what public spaces, if any, should be off limits? If you're trying to figure out where a terrorist attack is going to be coming from before it happens, how do you allocate limited resources and personnel? And then one question that I think I find frustrating that isn't asked more

frequently is whether adding to law enforcement's intelligence collection powers increases the likelihood of predicting violent activity.

So as we heard from the last panel, there are thorny First Amendment questions that come up but also significant privacy and equal protection questions as well. So how do you design a regulatory scheme that's both effective in countering the very real threat that we face but also minimizes these varied concerns? What is the ideal nature of those regulations? And who should be conducting oversight? And these are all things that we sort of touched on throughout the day, but now we have a great set of panelists here that are going to solve all the problems for us now. They've got all the answers. There are more detailed bios on them in your programs, but I'm just going to introduce them briefly before we start, and then you don't have to listen to me in between them.

So immediately to my life is Shahid Buttar who is the executive director of the Bill of Rights Defense Committee and a long time civil rights attorney, community organizer, and advocate. His work is focused on combating racial and religious profiling by government officials. To his left is Aziz Huq, professor of law at the University of Chicago Law School and Brennan Center alumnus by the way. He has written extensively on issues of national security and is currently engaged in a long-term empirical study of counter terrorism policing practices.

To his left is Philip Mudd who after a long and decorated career at the CIA became the first deputy director of the National Security Branch of the FBI and was later named the FBI's senior intelligence advisor. He is currently a senior research fellow at the New America Foundation's Counter Terrorism Strategy Initiative. And finally Suzanne Spaulding has worked on intelligence matters in both the executive and legislative branches serving as assistant general counsel at the CIA, general counsel of the Senate Intelligence Committee, and minority staff director for the House Intelligence Committee.

She's currently a principle at the Bingham Consulting Group. So with that, I'm going to turn to Shahid to get us started.

Shahid Buttar: Thank you, Emily. And thank you all for sticking around through the end of a long and fascinating day. Before I get into the proposed fixes, I do want to take a moment just to expand the frame in two dimensions. So first, for what it's worth, I'm actually more focused on dragnet surveillance and the dangers that it poses to society than I am to racial and religious profiling, though that obviously is also a concern. And in that context, I want to broaden the discussion. We've had a lot of conversation today about religious belief and the particular impacts of these domestic intelligence collection authorities on Muslim American populations.

But let's be real and look at the facts here. If you look at the terrorism defendant prisons in Marion, Illinois, and Terre Haute, Indiana, you won't just find Muslims there. You'll find a lot of white people, and a lot of them are non-Muslim. A lot of them have been accused of crimes relating to environmental advocacy. You also, at the moment, would find the FBI pursuing and dragging before secret grand juries in the Midwest 20 peace activists. And when we talk about intelligence information sharing in particular, the community that most comes to mind, the one that I think has been impacted most dramatically, is the Latino community.

There is a humanitarian crisis going on around the country because of information sharing between local police departments and Federal agencies. Not just ICE, but also the FBI, which has a particular role to play here because since localities around the country essentially started trying to opt out of ICE coordinated programs that entail intelligence and information sharing with local police departments, the Department of Homeland Security's maneuver was basically to do a spin move and say "We don't need the information from you – we'll just get it from the FBI."

So when we talk about the dangers of these kinds of authorities, I don't want the discussion of the impacts to be artificial cabined because they're much graver than we think, and let's just get into – I've talked about some of the communities that are impacted – let's just talk very briefly about some of the particular things that happened.

So the one risk is over inclusion, seeking information, particularly in an invasive way about people who do not actually represent security threats. And we talked about that in the context of the civil rights abuses of individuals in particular communities. Well, take a step back and think about what that does to our civil society. Linda alluded to some of this in her question after the last panel. These sorts of abuses don't just impact individuals, and they don't just impact communities. They impact entire ranges of communities.

Communities are networks, and when you inhibit legitimate First Amendment protected activity of the sort that the Bill of Rights was largely written to protect, it's not just the people that are impacted by the abuse who suffer, it is all of us. Those are public regarding protections, right? And so just think about the harms again in those broad terms. And then conversely, aside from over inclusion, there are all the national security problems that relate to under inclusion. So the danger of omitting potential threats like say people who assassinate doctors in the middle of church services in Missouri.

Those are threats that escape much of the counter terrorism and intelligence agencies' purview because they don't fit the race, faith, or politics model of the sort that we've been talking about today. There are other dangers beyond missing potential threats. One of them, and we talked about this too, is eroding the trust of communities and diminishing the human intelligence to which agencies have access. But there are further problems beyond that, too. So one is actually reinforcing the radicalization that, for instance, Representative King in the House claims to be concerned about.

The alienation of communities through the presumption of associational guilt is worse than merely chilling the exercise of legitimate First Amendment protected activity. There are potentially in any community disgruntled people who particularly lack access and may be driven, quite frankly, to things that they wouldn't otherwise contemplate. The genius of the First Amendment, in fact, has been that it has brought into the public sphere for two centuries grievances that might otherwise be expressed in other terms. And so there's an active reinforcing and cultivating the threat that we supposedly worry about.

And this last one I haven't heard much about. It's a little in the weeds, but follow me here – data mining. There is an active effort around the country, intelligence agencies at the state and Federal and local level. One of which is to identify the precursors that lead ultimately to violent extremism. This was the subject of the NYPD's report in 2007 that was horrendously and poorly argued, and other efforts since. Well, what is the point of that and how does it work? Well, you look at hits, you look at cases that supposedly demonstrate the concern, and then you look back, and you see what the precursors are.

And one of the concerns about the efficacy, or I should say inefficacy of data mining, in this context is whereas it works well in the commercial context, you can figure out when people buy milk what else they buy because lots of people buy milk. Well, not lots of people bomb things, so there isn't a large enough data set from which to extrapolate precursors. But there's a worse problem than that. Because when we contrive cases as the FBI does when it infiltrates faith institutions and then bribes heroin addicts and schizophrenics to participate in FBI initiated plots, you skew the data set.

So now we're drawing precursors from fake hits. The enterprise is not only inadequate in the present timeframe, but it is doomed in the long term because we have essentially polluted the pool from which we're trying to discern useful meta intelligence, the kind of intelligence that we can use in other cases. Okay. So having said all that, let's talk about fixes. So I want

to allude first to Professor Stone's argument in the last panel about the insufficiency of the First Amendment as a locus for protection.

And not only is it the case that, as Aziz mentioned, our constitutional law is under enforced, and not only is the doctrine unclear as Professor Stone noted, and there are standing barriers in access to justice being not adequate, but the recommendation, at least that I heard insinuated by Professor Stone's remarks, was to look to Federal policy as a remedy to raise rights above those constitutionally guaranteed. But the Federal policy here, the 2008 FBI Guidelines in particular, as far as I know, and I've asked senior people in the Justice Department, it's not even under review at the moment.

There are other Justice Department policies that are under review that have been under review for two years with no changes implemented. And so the effort to look to Federal policy as an area of salvation also strikes me as somewhat misplaced. If we can look to state and local analogs, and I think there is a lot of fruit here, particularly because the number of agents, if nothing else, are an order of magnitude, and then some, greater at the state and local level relative to their Federal counterparts. There are over 800,000 state and local police around the country. And the FBI, if you look at it as a Federal law enforcement institution, maybe is pushing 20,000 agents.

So there's a vastly greater problem with respect to the leveraging state and local actors, which is to say state and local regulatory reform efforts might offer one way to raise rights above the Federal floor while we fight the important battles that remain to be won in Washington. And just to think of a couple examples of this, right here in New York, the Center for Constitutional Rights did some FOIL litigation documenting the stop and frisk by the New York Police Department. It's been eluded to today, but just to spell out the facts there, a 9 to 1 disparity in the rates at which African Americans and Latinos are searched relative to white folks.

And when pressed about the demonstrable lack of utility in these stops and frisks from a law enforcement standpoint, the Commissioner of the New York Police Department's response was well, we're collecting valuable intelligence through these stop and frisks. And then when state legislation passes to try to restrain the practice, they do a spin move. And instead of collecting it electronically, they still collect it, they just do it non-electronically. So you see, even here in New York as a microcosm and reflected and replicated around the country is this problem of local police contributing to this Federally coordinated engine.

And the last reason I say that local and state reforms can be more availing relative to Congressional ones, or Federal ones, I should say, is that the

legislative branches are more accessible and empowered. Congress is inaccessible. You have to have either money or a ton of people to get to a member of Congress, and then they have to convince 200 colleagues. It's not true on city councils, often, they're much more accessible, and they have fewer colleagues they have to convince. As once you're able to get into the institution, the individuals are more empowered.

All right. So in terms of particular protections that we could impose, one broad one to look at are protections to address profiling in particular. Whether according to race or national origin, faith, or belief in the political sense. There have been attempts at this that, quite frankly, haven't gotten us where we need to go. In 2003, the Department of Justice issued guidance on the use of race in law enforcement that was dramatically under inclusive. There were formal exemptions for anything related to national security and border integrity, which is to say the policy is useless.

There have been attempts at Federal legislation that have not worked. The centerpiece of those efforts are data collection about the people that are impacted. So this gets back to Fritz's point about secrecy this afternoon. The first thing we have to do is gain transparency into who was actually affected by these kinds of data collection policies. I'm just trying to quickly wrap up here. With respect to other local things we can do, the first is address and enhance Fourth Amendment protections, particularly requiring individualized suspicion as opposed to associational suspicion, creating remedies in the criminal context.

The exclusionary rule inhibits the use of inappropriately gained evidence. But in the intelligence context, there's no analog. If there's intelligence that is collected inappropriately, or in worse cases where it's just inaccurate – Mike had talked about the intelligence in Virginia about racial enclaves being somehow pockets of radicalization – what happens to that data once it's out? There's no way to pull it back. There are 70 fusion centers and 100 JTTF's, plus the FBI Guardian database and whatever the NSA has. And I don't think those systems, to the extent they're interoperable, that it's a one-way ratchet.

And the last thing I have to say are the features of the '76 Levi Guidelines that have been eroded in the subsequent revisions, supervisory controls, sunsets for investigations, requirements for review by headquarters, the factual predicate to initiate an investigation. All of these things are on the table and should be adopted in a policy to fill these gaps.

Aziz Huq: Thank you, again, to Liza, Emily, Faiza, and the others at the Brennan Center for putting together this marvelous day. As Emily said, I am an academic. I am no longer a practitioner like my colleagues on the panel. And, therefore, I don't have daily exposure to the practical problems

involved in domestic intelligence collection or in the consequences of such collection. And so I think the safe inference for you as an audience to draw from that concession is that I don't know anything, right? And I excel in saying that in many more words than is needed. If academics have a comparative advantage, and I very frankly am not sure they do, it's in their ability to reflect at more length on the implicit logic of a regulatory structure.

It's in their ability to try and distill the ambient reasoning of the law. And so my limited goal in these comments is to make a suggestion about a new design principle, or a design principle that's at least I think new to these discussions, that might aide in our thinking about the design of domestic legal institutions, specifically by being somewhat more clear about the value of privacy. It's a design principle that I think helps us identify and think about some of the blind spots, particularly in the constitutional architecture, and perhaps also in the statutory and regulatory architectures. And I should say upfront that to the extent that there is an insight here, it is not new, and it is not mine.

I'm drawing inspiration from my colleague at the University of Chicago Lior Strahilevitz, who has written about how the value of privacy is protected through the tort law. And there's a scholar at Stanford University called Helen Nissenbaum who has written more abstractly about the philosophical value of privacy. But I think the insights that one gains from their work are usefully arbitraged over to the national security context. The core intuition that I want to elaborate is this, our dominant notion of privacy is far too limited to do the necessary work in thinking about the effects of regulation of domestic intelligence.

That dominant conception of privacy is a classical, liberal one. It traces its roots back to the thinking of John Stuart Mill. It is a discrete and individual conception of privacy. Privacy, that is, is imagined, presumed, and protected as a zone, almost a physical zone, of immediate, individual autonomy that clings close to us as the atmosphere clings close to the earth. And as a result, judicial responses and social mobilizations around novel incursions on the values that privacy might protect either fall short of being effective or fail to capture the public imagination because they are insufficiently responsive. So let me try and unpack that point mostly by talking about the law. And I'm mostly going to talk about the constitutional law because that's what I happen to know the best.

The concept that lies behind the Fourth Amendment's protection of privacy for almost 200 years after its enactment in 1791 was the protection of a physical space that was close to the person: one's literal, physical person, one's pockets, and most importantly, one's home. It was only in 1967 in a Supreme Court case called *Katz* that the justices extended the

right of privacy against telephonic surveillance, and it announced the standard that Geof Stone mentioned, the reasonable expectation of privacy standard.

You have a Fourth Amendment interest whenever you have a reasonable expectation of privacy. Now, as ought to have been obvious to the justices at the time, but clearly wasn't, what expectations are reasonable is a function of what the law is. As economists like to say reasonable expectations are endogenous to the content of the law. So it's entirely circular to look to reasonable expectations to determine what the law ought to be. So even at the beginning, we have this an individualized focus upon reasonable, individual expectations that is intellectually incoherent and that an important part has been carried through into the Federal statutory structure.

So if you look at statutes like the 1974 Privacy Act, you don't have this problem with reasonable expectations. But you do have a focus upon individuals. Privacy with important exceptions in the case law, I should say, is turned around, an individual concept. But that discreet and individual concept to privacy I think is an insufficient response to the manifold ways in which government predictably looks inside the domain of an individual life in ways that might inhibit that individual's robust participation in political and social life in ways that they choose to participate. So consider the government's options if it wants to peek inside my life, me personally.

So I live in Chicago. Let's say I drive to work every day, and I drive on a highway where there's an easy pass system. So I flash my easy pass at the beginning of the system, and I flash it at the end of the system. I sit in an office, which has shockingly thin walls. And so most of what I say in the office can be overheard by the person next door, who happens to be Geof Stone, but he's a well-known government stoolie. And I do all my research on a computer and a telephone and an internet server that is provided by my employer, the University of Chicago.

So under current law, the government can with the relatively undemanding process that is associated with an administrative subpoena obtain the electronic tollbooth records that show when and how I've traveled, the bank or credit card records that show when and how I've purchased gas, where or how I've eaten outside of the home. Because I live in a state that's in the seventh circuit Court of Appeals, the government can attach a GPS device to my car and monitor my movements. Whatever jurisdiction I lived in, as has come out in previous presentations, the government can ask my neighbor for his report of what he has overheard in my office.

They can make the same request of my spouse if my spouse is willing to divulge that information, of my neighbor, or relevant here, of fellow congregants at a religious institution I choose to participate in. The government can seek out my correspondence in research and secure information, as has been pointed out, by enticement or threat. And it can approach my employer, and because I'm not a student, who's covered by FERPA, the Federal statute that protects privacy rights in education. It can secure from my employer with, again, relatively minimal process the contents of my email and other records that may be on my desktop computer.

Now, the point that I want to draw from this, and I'm going to draw two points on this, and they're not about the specifics of the Stored Communications Act or any other Federal statute, rather they're conceptual points. The first point is that privacy is not an individual matter, it's a relational matter. In social and political life, no one is an island. We are exposed through our friends, our work colleagues, and most pertinently here, our co-congregants. We expose ourselves through work, through friends, work colleagues, and co-congregants. Sociologists since the early 1970's have pointed out the crucial role that not just close ties, ties that may be protected by some kind of legal privilege, but weak ties play in social life.

There's an enormous body of work on the role of weak ties in social life that is entirely not registered by the law. Dependent on wide networks of people we know limply, so to speak, is not just an economic and social strand, it's a privacy weakness. We are further exposed by our reliance on commercial third parties, credit providers, ISP's, commercial parties that maintain historical records about us. And yet the Fourth Amendment doctrine draws a sharp line between my interest in information that I hold myself about myself, an interest that a third party, be it commercial or non-commercial, holds about me.

Information that I hold about myself is protected robustly under the Fourth Amendment. Information that is held by a third party, be it an individual or a commercial entity, gains no constitutional protection at all. And it gains some statutory protection, but I think the statutory protection ought not to be overstated. As a consequence, our privacy is not really an individual function. It rather rests in the hands of friends and strangers vulnerable to whatever inducements, suggestions or threats the government may have to offer. The second lesson that I would draw from my hypo about my own vulnerability is that the relational aspect of privacy is magnified by social and technological changes that have dramatically changed the data trail that people leave in their wake.

There are now a range of largely commercial, but not entirely, entities that hold deep pools of information about us. Our employers, our creditors, anyone we transact with on a business basis. Technological change means that there are manifold ways for the state to use that information to draw insights about individuals that would not have been possible in the past, specifically through aggregation. That is while the individual breadcrumbs of our electronic data trail through the world, may not be revealing, when aggregated and analyzed, and Shahid referred to this obliquely, they can be quite telling. They can be quite telling about things that many of us would like to keep to ourselves.

And following Moore's law, we know that it becomes cheaper every day to do that aggregation. And, again, the constitutional law has said almost nothing about aggregation. There are a few hints in a 1970's Supreme Court opinion called *Whalen v. Roe* that there are statutory requirements about minimization, although it's hard given their opacity to say that they provide a clear assurance of privacy. Combine the law's failure to recognize the reasonable expectation of privacy that we have when we disclose information to a third party along with the power of aggregation, and I think it's easy to see that the prevailing model of privacy and protection is inadequate.

To give a very straightforward example, what good is it to prohibit, as Congress did, the Dopper TIA program if the government can, simply through the purchase of commercially available data, replicate that program. The law, in short, has failed to keep up with changes to technology and social morays and remains entangled in a limited and limiting conception of privacy. I should close by saying that I don't think that having identified if you think that this is a problem, and maybe you don't, if you think this is a problem, it's not clear how one changes it. Courts are not going to change the dominant concepts of Fourth Amendment privacy.

Congress probably isn't going to. Likely, where change, if change happens, starts is in the changing views of the public and elites. And I think it's perhaps in discussions of this kind that that change first gets seeded.

Emily Berman: Thanks, Aziz. So now that we know that the constitution provides absolutely no help in regulating these issues, Philip Mudd, what should regulation look like?

Philip Mudd: Well, as a former CIA official, I think we should just make up the constitution and move on from there.

Aziz Huq: That's okay. That's what constitutional law professors think.

Philip Mudd: I do notice we have a Brit lecturing us on constitutional law, but we'll pass that. Let me be serious for a moment, and that was brilliant. And I know this wasn't by design. I won't give you that much credit, Emily, but what I'm going to say follows not by design, just on what my predecessor said about law. But I'm going to apply that to practically what I saw in sitting in nine years of morning and evening threat briefings at the CIA and FBI. In close, since this is a semi academic environment, in maybe offering some homework, and real homework, research and study that I might think would be helpful to government practitioners.

I confess, I do feel as someone who has served both in CIA detention and rendition programs and in the Institution of FBI intelligence programs that I should have an escort walking out of this building. But let's leave that at that. I want to talk initially for just a moment about some concepts, and then quickly transition to some practicalities and close, again, building on some of the questions about gaps in law with some homework. So three quick segments here, and I should be done in 10 minutes or less. The first in concept, you look at how the threat evolved. When I returned, I was a White House and CIA detailee to the White House on 9/11.

And the only time I saw the DC government efficient was when I ran out of the executive office building on 9/11 without my wallet and keys. I didn't laugh about it them, but laugh about it now, but they towed my car within 12 hours, the DC government, because it obviously was parked on White House property at that point. And I remember even then thinking the DC government is not renowned for efficiency, but today on 9/11 they have efficiently not defended against the threat, but they did tow my car and charged me $50.00. But I remember leaving there for CIA after a tour as the referent on the diplomatic group that installed the Karzai government.

And I came back to CIA in early 2002, and for a couple of years was one of the two people briefing the now renowned threat matrix, matrix to Director Tenet every night at 5:00. And the first snapshot of threat is that most of those threats were related to the Al-Qaeda, what we call now the Al-Qaeda core organization. It was questions about whether operatives were sent from the tribal areas of Pakistan or sent from Al-Qaeda affiliates in places like Saudi Arabia to conduct for their tax. And I remember the sense of the unknown, especially on Friday nights, which are the nights I remember the most.

Remembering that even years in, you couldn't know whether that core organization had sent people here that would lead to an attack where a child would never see their parent again. I just remember driving down the parkway every night saying will I be involved and responsible for

something that leads to a child growing up without a parent. But that threat was affiliated with the Al-Qaeda core organization. Now, to close on the threat piece in the transition in threat piece, what do we see today? We see Hassan in Texas. He had connectivity with al Awlaki, so do thousands of people.

He also had access to a weapon. By the way, he was in the US military, and secondly, that's a constitutional right. So he has a free speech right to talk to somebody, and he has free speech right to have a weapon. He's ideologically motivated by a core organization but not directed by them. And you've all seen, I don't like the term home grown, this is a global Jihadist phenomenon, but there are people who are not connected operationally with Al-Qaeda, and the lion share of people today conspiring to conduct attacks are people who are only ideologically inspired. That is they might look at a website or talk about something. That's a speech issue.

So the transition to close on this piece of the thread is from a core organization that you can target with intelligence resources to a guy who is an American citizen with a uniform in Texas. Number two, and to close on conceptual issues. Director Tenet called me in the summer of 2005, I had testified with him earlier, and there was a great deal of media pressure then on the Bureau and congressional pressure, public pressure, and White House pressure, for the Bureau to continue transitioning from purely law enforcement to preventive. And there was a law passed in 2004, the Intelligence Reform Act, that mandated that the Bureau move on. And I became the first ever deputy director of the National Security Program at the Bureau.

What did the law say? There are a lot of lawyers in this room, and this has been a frustrating day for me, I confess. There has not been a lot of conversation about law. What did the law say? It said in 2004 that the Bureau must have a preventive counter terrorism posture. That means stop things before they happen. That means by definition, you cannot always tether investigations to proof of criminal activity. It's not a choice by the Department of Justice, by the executive branch, and by people like me.

It's what we were directed to do by law. Let me make this an uncomfortable conversation. If you choose to be preventive, we didn't choose, we were told to, by definition, if you are preventive, there will be people dragged into those investigations who did not do something wrong. I wouldn't have said this if I were a government official still. I quit a year ago. But if you find 100 percent of people in your preventive operations who you can convict, you're not doing your job. What happened?

I testified, one of the only times I returned to the government in the past year--six years, seven years, after the 2004 Act--on the Fort Hood event, an individual who operated alone and then probably until that morning or maybe a few days earlier made a decision in his mind, which I can't access with the internet, with a phone, or with anything else, to commit an act of murder. What did we have on him? He communicated with a bad guy. He had a weapon. And he thought about killing people. What did the investigation say seven years after the Intelligence Reform Act? I'm not speculating among lawyers. I'm telling you what the legislature of the United States said and what they dragged me up as a US citizen, now private, to talk about.

They said the top priority of the Federal Security Organization, and the FBI is preventing, and the FBI did not prevent this, and they are not yet intelligence driven. So if you want to talk about it, and I heard a phrase earlier about whether adding intelligence increases our ability to prevent, we did not have an option. It's what the law says. I ain't no lawyer, but I'm a servant of the US government in the executive branch who responds to the will of the people. So you have a threat this chance, you have an individual, and I cannot predicate that individual on core Al-Qaeda, and you have a law that says if you wait until something happens, we're going to put your ass in a sling.

We don't care about gang violence. We don't care about drug violence. If one dude who seems to be a terrorist kills people when there are 15,000 murders in this country every year, you're coming up to testify.

All right. Let's transition to some practicalities. I need a drink, by the way. And by the way, Emily, I'd like to point out that the organization here paid me as I transitioned to the private sector in a huge company called Mudd Management, one person, paid me $0.00 to come up here. So all this energy is for nothing, and that really pisses me off. So let's transition to talk about how you apply the principle of being preventive in a threat that's more individualistic in some circumstances that we've seen over the past year or two.

Note that there is a mention by Emily about factual predicate. There are factual predicates for every example I'm going to give you. The problem is they're predicates for behavioral activity, they're not predicates for an individual. If you wait until you find an individual, you've already waited to be a law enforcement organization after you predicated a criminal act or the conspiracy to commit a criminal act. So think about three or four examples, and I'll close in a second on some homework. I mentioned one, Hassan. He had a weapon, US military guy, that makes it even harder, and he communicated, and I use that word advisedly with the terrorists.

A week earlier, if we had gone up on that guy, and he hired a lawyer, what would that lawyer have said? By the way, remember, he's an academic doing research. He would have said he's doing research. He has the constitutional right both to talk to people and have a weapon. The day he committed an act of terror – I don't think it was an act of terror actually, I think it was just murder – that results in a Congressional investigation. Because we failed to be preventive. In the space of minutes, we went from a civil liberties violation to a major national security catastrophe because we weren't preventive.

Think about a piece, and Andrea Elliot, is a brilliant journalist – I hate to say this – no journalist is brilliant – she's very good. Has a piece in the *New York Times Magazine* that talks about, a fascinating piece, that talks about an individual who is a prominent American Muslim and talks about an institute, he's involved in, Al-maghrib and talks about individuals who in my world were very prominent individuals like Daniel Maldonado and Abumutallab from Detroit. So my first question is what do you do about Hassan before it happens? Is it okay because he has a weapon and is talking to someone to look at him?

I guess you could call that behavioral profiling, by the way I dispute religious – I never heard of religious profiling in the Bureau. So we can discuss that, I'm throwing it off the table. I never heard anybody say let's go after somebody because he's Muslim, and I never heard anybody say let's go surveille a Mosque. Mosque is a building. If bad things are happening there, I personally as a US citizen would go into the Mosque. We don't go into buildings, so we can talk about it if you want, but I'm not going to address it because I didn't see it. Four and a half years, every morning threat briefs, three attorneys general, one FBI director, five days a week, I never saw it.

So let's talk about what I did see. Hassan is one. So let's talk about the institution that's in the New York Times Magazine this week. So you see some people who are involved in high profile terrorist, not only investigations, but who are convicted now. Would you go look at this institution? Would you say that's enough predication, that's a fact that people coming out of this institution, Al-maghri, have been involved in terrorism. Is it appropriate to go look at it now? Is that appropriate predication? I don't want a waffle. I want a yes or no. I'll make this easier in a second. I'm just very excited now.

Third, let's try non-US persons: Saudi students. Fifteen of nineteen hijackers in 2001 were Saudis, and we just had a Saudi arrested in Texas a month or two ago, a Saudi student. The last I heard, I'm guessing there are probably 18,000 or 20,000 Saudi students in this country. We have the most significant attack on US soil ever conducted by 75 percent Saudis,

and we have an indication, a fact, from a month or two ago that there is still a problem with the Saudi student population. Would it be appropriate to put human informants within major Saudi student populations in the United States? Do you think that's okay? There's predication. We're supposed to be preventive.

And as George Tenet once told me, there ain't no learning the second kick of the mule. I don't want to testify if there's another Saudi attack in this country saying well, we didn't have evidence that further Saudis were conspiring, so we chose not to do anything. I'm not saying I would support human source operations. I'm saying the question is tough. And finally, let's take something that Andrea also worked on, Somalis. Let's say you were looking in 2005 or 2006 at fund raising operations in the United States to support the Shabaab organization in the horn of Africa.

And let's say just based on a question, you said if there's that much fundraising, perhaps that we don't have criminal information on this, perhaps there's also recruitment for kids to go fight. Maybe we should go ask human sources to look at that. I can tell you in 2011, I suspect the parents of the kids who went and died in Somalia would say that's okay. So here are the questions for you as we close. Intelligence typically is based on two threads, that is human sources and technical sources. I've given you examples that relate to the emerging threat that is individuals, not a core organization, and that is be preventive, not just responsive.

Hassan is a technical issue. Is it okay to surveille the internet to look for people who are communicating and speaking, First Amendment right, with a terrorist. You want to pay for that? And if he's got a weapon, do you want to put a human source on him? Is it okay if you have reporting showing that a recently emigrated community, that is Somalis in Minneapolis emigrating after 1991 – 1992 are involved in fundraising to say it's a fair question for a preventive organization to assume that if there's that much fundraising, there is also recruiting. Do you put a human source in that community? Yes or no?

I heard a lot of conversation today, but let me tell you something, we're not stupid in Federal government. And there ain't no learning the second kick of the mule. So the question is when the law, it is not a choice of the Federal Bureaucracy to take these, the law says be preventive, and when you're not, even as a private citizen, you're going to testify for why you missed somebody talking to a terrorist over the internet. When the law says that and when the threat shows you that the problem has metastasized, what will you do? Thank you.

Emily Berman: So I need to interject. First of all, I hope we make you feel more welcome than actually wanting an escort out of the building. And I just want to say

we do very much appreciate having you here. We made an effort to have divergent viewpoints because –

Philip Mudd: Don't worry.

Emily Berman: I'm not worried. I just want you to understand that we're very appreciative of your presence. We've tried very hard on a couple of occasions to get people from law enforcement, from intelligence agencies to come and speak with us, and they're very reluctant to do so. So we are appreciative when someone comes.

Philip Mudd: Why do you think that is?

Emily Berman: And as Aziz said, I think if we're going to find solutions to these questions that you pose, which are very difficult, and I concede that freely, this is how we have to start doing that is to talk to people that we disagree with and try to figure out what we're going to do.

Philip Mudd: And to be quick, I should have closed with a point. I meant honestly what I said about research. I think it would be interesting to look at – I don't think modeling religious behavior is appropriate, and I agree. I hate to say this, but I forget the phrase that you used about – you used aggregation, but about looking at mass data. I don't think that stuff is that helpful. But a couple of things I look at is what behavior – if you're told to be preventive literally, what behaviors do you think are appropriate under the law. I've not seen any work on that, and I divide that into both technical information as surveilling the internet. Also, what's appropriate for human sources.

And the last thing, I've seen overseas, I've never seen it done here, but since you brought me up here, I'll give you a problem. It would be great to see a place like NYU do something I've seen the security services do overseas, and that is switch roles. Create a scenario where the community plays – the Federal Security Organization plays the community. Go into something like the Somalia case and play it out for a day. And my friends overseas, and believe it or not a year out, I still talk to a lot of security services, have told me that those scenarios by an outside party are extremely useful for trust.

Emily Berman: So with that, I'll turn to Suzanne Spaulding.

Suzanne Spaulding: What was I thinking going after Phil? And Phil, I know that when you kept talking about the consequence of this is that you get hauled in front of a Congressional committee, and I know that you don't mean to imply that you're somehow intimidated by going and testifying in front of Congressional committees or that somehow that weighs heavy on the

scale. But I think what you're getting at is that that is a reflection of society or at least Congressional expectation. Right?

Philip Mudd: That's correct.

Suzanne Spaulding: And so I think that's a good place to start, which is to say I think we are not going to make much progress, certainly with Congress or with the American public, until we can really hammer home the reality that counter terrorism is not an exercise in risk elimination, but an exercise in risk management. And it's really hard, it's politically almost impossible to get that across. But until we do, we're going to continue down these counterproductive paths chasing the myth of risk elimination.

And so everything that happens will generate, as Phil says, an after action report that says something went wrong because if we just did everything right and what the American public hears is if I just loosen the reigns enough on the Federal government, if I just give them a little more authority, then I can be perfectly safe. And I think part of what you're suggesting, and certainly Brian Jenkins I think has suggested with regard to someone like Hassan, is that you can give us all the authority in the world, and there is still going to be people out there that we cannot stop. And I think that's really important – it seems sort of obvious in a way, but in some sense, we've never internalized that.

And our public officials need to say it much more often. Some of them have come close. I've heard Janet Napolitano say this in a small room. The notion that your government is doing everything it can to prevent another terrorist attack, but the reality is there is no 100 percent guarantee. And the important thing to remember is that if there is another attack, we are a strong and resilient nation, and we will go on. And that is a simple message, but for politicians, it's incredibly hard. But until we do that, we're going to be continuing to chase this impossibility and making these demands on our intelligence services that are going to drive us in really counterproductive ways.

And of course, we can do surveillance on everybody who is talking with known terrorist because we can be surveilling the terrorist end of that communication and, in fact, that is how we got Hassan's communications, and that is apparently, according to the Senate's report on Hassan, how we came across Zazi. So that is there. I wanted to talk about, and some of this is the homework assignment that you gave, I think Congress can be helpful. I wanted to talk about the role of Congress in all of this as part of the regulation and the governance and the oversight. And as someone who has worked for both the Senate and House Intelligence Committees, I have to apologize for Congress's failures and inadequacies in this realm.

I mean, it's really very difficult. But I think there are some fundamental principles. One is that Congress needs to understand the differences between criminal investigations and intelligence investigations. And why we need more safe guards, not fewer safe guards on intelligence investigative authorities as I've watched with distress as someone who has spent 15 years or so working with FISA, the Foreign Intelligence Surveillance Act, in the realm of intelligence investigations and operations. As after 9/11, more and more authorities from the criminal context migrated over into FISA.

And instead of tightening safe guards or building in additional safe guards, we lost safe guards in the transition, and it's really troubling because intelligence investigations don't have the built in safe guards that prosecution brings to the criminal context, which is so incredibly important. So it's a natural kind of built in oversight mechanism that law enforcement officers know that if they're pursuing this subject that might be susceptible to criminal prosecution, if the abuse their authorities, they're going to screw up that prosecution. That isn't there always in intelligence investigations if they're not focused primarily on prosecution, which they often aren't.

There is obviously the secrecy, and then there's the narrow versus broad focus. I remember being on the Senate Intelligence Committee after the Oklahoma City bombing. We had people come in to us, citizens, who told us stories about this John Doe No. 3. That there was a third person who was involved, and they had all these elaborate evidences as to why. And we would dutifully send it over to FBI and the Department of Justice, and they said to us we don't want to hear about this. We're not interested in whether there might be a John Doe No. 3 frankly because we're far along on our case on this. We're getting ready to present our case against Timothy McVeigh and against Terry Nichols, and the last thing we want to do is introduce some element of doubt in the jury's mind.

So criminal prosecution, the contrast between that mindset and intelligence collection could not be starker. But it's also the constitutional framework around criminal investigations. Our constitution requires that our crimes be defined very specifically. They can't be over-broad. They can't be vague. So that we understand and we know which side of that line we are on because the concept is if you understand where that line is and stay on the right side of that line, the government is not going to intrude into your life. Well, after 9/11, we moved from "criminal predicates" to "suspicious activity," which is not defined at all.

And now you have no idea what activity that you engage in might bring government scrutiny to bear. So again, very stark difference there. That doesn't mean that we shouldn't have some intelligence activities going on

that are broader than criminal investigations. It simply means that you have to recognize the risks and build in more safe guards rather than fewer safe guards. And I guess what's so concerning and what I hope Congress will look at, and I said I was going to talk about homework for Congress, I really am not convinced that they have studied these attorney general guidelines and really probed sufficiently into what they provide for.

And we've touched on it a bit today. But the guidelines discussion about what you can do and what assessments are all about, particularly in the context today of this big push towards understanding radicalization, is really troubling. So in Denis McDonough's speech, which he gave last week or two weeks ago, he talked about how important it was to improve their understanding of the process of radicalization that leads people to terrorism. And he noted that they've set up entire analytic units at the Department of Homeland Security and NCTC to help them understand this process of radicalization. So what might they be doing under that rubric?

So here is what the attorney guidelines say with regard to assessments. "Assessments may be undertaken proactively with objectives such as: obtaining information on individuals, groups, or organizations of possible investigative interests because they may be targeted for attack or victimization by such activities." So assessments can be done on people who you think might be targeted for victimized or radicalized. And that includes this whole list of authorities as we've talked about today, including the recruitment of human sources, use of online services and resources whether nonprofit or commercial, and we just talked about data aggregation and the weaknesses in terms of the current understanding of third party records, which I could not agree more needs to be re-evaluated.

And this language in Section 215 and elsewhere in the Patriot Act that came in after 211 where we provide these even more intrusive authorities to protect where there's an investigation to protect against international terrorism has always troubled me. It's not an investigation into international terrorism. The language is to protect against international terrorism. So I think some hard questions need to be asked of the government and the FBI and DOJ about how they view the use of these authorities under assessments. National security letters used to be limited to FBI. Only FBI could issue national security letters and, of course, as we know, even the FBI's authorities under national security letters were broadened after the Patriot Act.

But also, what was added is the authority to use national security letters by any agency in the government for analysis, that's engaged in analysis, of international terrorism. So now these can be issued by CIA, by DOD, by anybody. And so Glenn Fine does great work at the Department of Justice looking at the use of NSL's and uncovers all kinds of problems, which

Congress pays a lot of attention to. And I want Congress to ask the DNI's IG to take the IG's of the intelligence agencies and do a joint look at how they're using national security letters in this context. These are important questions and things that Congress needs to do. Sting operations. I think Congress needs to take a very careful look at how sting operations are being used. We had in 2010 according to Brian Jenkins, and I would recommend to you his report "Would Be Warriors," and I know he's updating it.

But it gives a really clear-eyed view and disaggregates the nature of the threat. He says we had six cases in 2010 that actually involved plots inside the United States. Three of those were sting operations. I think we have to look very carefully, and I've read in the indictments they ask these guys right as he's about to push the button to blow up the fake bomb "Are you sure you want to do this?" And that's I guess supposed to keep it from being an entrapment. But think about these young kids who are out there online. I mean, what Brian Jenkins concludes that so many of these are stings and that so many of the cases never got as far as actual plotting is that they're a lot like my son who can't plan his way out of a paper bag.

I mean, if any of you have sons, you know what I'm talking about. I don't mean to minimize the threat, and I don't mean to trivialize this. But I do think that Congress needs to pay careful attention to some of these issues that I don't think are getting enough attention. I would say, and then I'll stop, I'm going to pick up on a couple of things that have been mentioned before, and then I'll stop so we can get into the discussion. Aziz said information that I hold about myself is rigorously protected under the Fourth Amendment, and this is one of my pet issues is that Section 215 as modified in the Patriot Act no longer relates just to third party records. Not only does it not no longer relate to just business records, it no longer relates to third party records.

It says they can demand any tangible item from any person. Now, there is some language later, and I looked to get the quote, but I couldn't find it in time, about that it has to be information that could be legally gotten under a subpoena or something. I mean, I think there's some reference to it has to be constitutional. But again, it's all done in secret, and we don't know how these things are being applied. And I would say on the third party doctrine, the Smith case, which is one of the two or three fundamental cases that established the third party doctrine had to do with phone numbers. If you go back and read the case, the court says getting phone numbers just isn't that big an intrusion.

You can't even connect a name with the phone number. And that's how dated that third party doctrine is. So well overdue for a look. I'll stop there so we can have some discussion.

Emily Berman: Where to begin. So I couldn't agree more with Suzanne that the expectation of 100 percent prevention is incredibly unrealistic and places an unfair amount of pressure on law enforcement to be psychic about what's about to happen. But if, as you say Phil Mudd, the mission of the FBI is it's mandated to act in a preventive fashion, how do you decide what to investigate? What do you base decisions on, investigative decisions, if you're supposed to be figuring out what's going to happen tomorrow?

Philip Mudd: Is that rhetorical? Well, let me give you a couple of examples. And again, they relate to – I didn't see ethnic or religious profiling – what I saw was looking at past behavior, which, again, is sort of a fact in saying do we take a message from that? And a couple of examples would be once you see X number of kids between the ages of, let's say 16 and 35, 35 is not – well, in my world, it's a kid, but 16 and 35. Let's say you buy a one-way cash ticket to Pakistan, and let's say they travel – I'm not saying we do this. I'm not being coy. But for example sake, let's say they travel three times in the course of two years for at least one trip is a minimum of 30 days. In other words, I've seen a lot of activity in Europe, the United States. That's not a bad indicator that maybe somebody, a one way ticket, not traveling with a seat companion, paid cash, maybe bought the ticket less than 60 days or 30 days in advance of the travel. Maybe he's going out for some training.

Now, you would say is that appropriate in terms of behavior to look at someone. And I think that's the kind of problem that I saw in my experience. The other problem, I mean, the real challenge was not investigations. My experience in Federal law enforcement as a CIA detailee was as an American citizen, once somebody is predicated, that is there's information that suggests that they're involved in conspiracy, the Federal law enforcement services are excellent.

So you have a foreign service say we got a bad guy who we know traveled to Pakistan for weapons training, and he just called your dude. I can tell you, I didn't worry about that. The question I had was who is not on the investigative sites so we can be preventive. So one would be looking at behavioral activity. The other even tougher would be to say okay, we have horrific attacks on a Jewish center and hotel in Bombay that led to a lot of people dead in global coverage in Mumbai in 2008, I guess it was. And that's conducted by a group called Lashkar-e-Taiba of Pakistan that increasingly used to be a localized, a regional group, now it's adopted the Al-Qaeda sort of targeting methodology of "let's go after Jewish targets".

Should we ask the question of how confident should we be that there's not a Lashkar-e-Taiba presence in the United States. That's very difficult to

answer, but I think it's legitimate for a security service to ask. Now, the questions I how do you execute that? And I think the laws suggest that if not at least think about it, you should do something about that. Now, we could talk about how you execute it, but it's really hard because there are a lot of Pakistani citizens in the United States – I mean, they're not "Pakistani-Americans." I hate hyphenated Americans, they're Americans.

But Lashkar-e-Taiba now is a global terrorist group, and there's been American, David Hedley in Chicago, Illinois, and he's got a co-conspirator out there, who has been involved in conspiracy to commit murder that resulted in many people, many dozens of people murdered. So what do you do? And that's the sort of ambiguous, and that's why I wanted to challenge –

Suzanne Spaulding: In that case, we had some warning signs early on for David Hedley?

Philip Mudd: I'm not talking about Hedley. I'm saying you look at that and say boy, is there a Lashkar-e-Taiba type of problem in the United States? I mean, and if you get a Lashkar-e-Taiba member in Los Angeles next week who does something, somebody is going to call you up and say you've got to be kidding me. You never – you didn't know about a network, but you never asked yourselves after Mumbai whether we had the same manifestations of a south Asian militant problem in the United States as they see in Britain and Pakistan and India? You got to be kidding me. And at that point, they don't care about "Well, I'm sorry, but under the Federal Guidelines…" – they don't care.

Suzanne Spaulding: But Phil, there are plenty of things that you can do at that point. I mean, certainly, you've got broad authority to be conducting electronic surveillance of suspected members of Lashkar-e-Taiba overseas.

Philip Mudd: I disagree. Lashkar-e-Taiba is a prohibited organization, that's a predicated act. We're talking about looking at people before they are predicated for a criminal violation.

Suzanne Spaulding: But you're talking about trying to figure out if there are affiliates or members of or sympathizers with a known terrorist organization many of whose members we have identified. And if we aren't conducting electronic surveillance of them, I don't know what – somebody should be fired. And if they're making contacts with people inside the United States, that's a good place to start, isn't it?

Philip Mudd: No.

Suzanne Spaulding: Why?

Philip Mudd: Well, you're making this too easy. What I'm saying is if someone is affiliated with an identified terrorist organization that's designated by the United States, I don't have a problem. That person is engaged in conspiracy with a terrorist organization. I'm saying we don't know – I'm speculating. Let's speculate in 2008 we don't know if we have a Lashkar-e-Taiba presence here, but we know we have significant Paki –

Suzanne Spaulding: But you start by seeing if there are communications from overseas into the U.S. –

Aziz Huq: Why don't we change the hypo to make it more of Suzanne's problem. Or not your problem, but to pose what you're trying to pose in a sharper way. So I think that people generally have no objection to the idea of behavioral predicates in that there are some pattern of acts that this person has done that has been predictably identified across a series of historical instances in the past leading up to an act of terrorism. Those I think are in a domain of broad consensus, as are the cases I which by and large the entity to whom the person has connections to has been designated either under Title 8 by the secretary of state or under IEPA by the president.

Where I think the domain of difficulty or disagreement is and where I think it may be that this domain of difficulty and disagreement doesn't reflect perhaps current FBI practice, perhaps it reflects more what's happening in Congress on the one hand and what's happening at the state and local level is the idea that you can either take mere religiosity or some proxy for it as a sign of risk, as a proxy of risk. And it may be the case that – you've been very clear that that's not something that you think the FBI has done, that's fine – but there is I think a legitimate, maybe it's legitimate, but there is certainly a public debate about that question today in part because of the [Rep.] King hearings.

So that's one set of problems. The second set of problems, and I think this is really another way of putting Suzanne's question, is imagine you have an organization that is not designated. Take an organization like Hizb ut Tahrir where you have historical evidence that people have transitioned through Hizb ut Tahrir to other organizations over committed acts of terrorism in the past, but Hizb ut Tahrir is an organization with tens of thousands of members and where the number of people who made that transition may be very low.

But the rate at which Hizb ut Tahrir members commit terrorism is substantially greater than the rate at which people in the general population commit terrorism. Is that alone enough to begin an investigation of somebody who self identifies in the United States as a member of Hizb ut Tahrir. Is that a way of getting at your question?

Suzanne Spaulding: Well, I think it is a harder question than the question that Phil posed.

Aziz Huq: I think he does pose easy questions, himself. You've got to pose hard questions.

Suzanne Spaulding: Right.

Philip Mudd: Can I defend myself here?

Suzanne Spaulding: But my point was simply that you don't have to start by sort of looking out at the populous and saying how am I going to find them? In the cases that you're going to detect, it seems to me, you're going to have communications, and you're likely to have communications with people overseas who are probably on your radar screen. Now, the harder cases, you don't have that. But the case you posed, you would have that.

Aziz Huq: So how would either of you answer the Hizb ut Tahrir question? Is that a sufficient piece of information to begin an assessment?

Suzanne Spaulding: Under the attorney general guidelines, it certainly is.

Aziz Huq: A citizen in the United States.

Suzanne Spaulding: Is your question should it be?

Aziz Huq: Should it be.

Philip Mudd: Two responses, let me do that, and then relate it to Hassan because we always look at Hassan and say we should have seen him. I want to reverse it and say *how would we have seen him*. Practically speaking, I don't think as a practitioner that would be possible. I would be looking at that saying if we have a roster, given the experience and behavior in, for example, Europe, if we have a roster of Hizb ut Tahrir guys. There's not 20,000 here. There are 12,000 or 13,000 that are doing public corruption. They're doing white-collar crime. They're doing kiddy porn, which is by the way the worst thing I saw at the Bureau.

There's an epidemic of kiddy porn in this country. They're doing drugs. They're doing border stuff. They're doing people at the City Hall who are skimming money. So Hizb ut Tahrir, you're also looking at Hezbollah. You can't look at that many people. You might say are there people in Hizb ut Tahrir who are this age? I'm not saying you would do this, but as a practitioner, I might say this age. Maybe they've accessed beheading websites. Maybe they've been to Pakistan four times in the last two years for a minimum of 30 days, bought a cash ticket one way, didn't travel with a companion. They I might say "That's interesting." I'd be calling the

lawyers in and saying is that okay? But I think just generally, about Hizb ut Tahrir as a practitioner, I'd say "Man, you're going to get too many people. I don't have the resources to do that."

A quick close on this. We're too quick to say on Hassan okay communicated with a known Jihadist, and he had a weapon, let's go reverse. al Awlaki talks to thousands of people. To find Hassan, and I'm not being facetious, let's say you're going down and who has talked to him from the United States, not talked to, but at least tried to communicate. My guess is thousands, and I'm just guessing. I can say this because I don't remember what the intelligence information is. So thousands of people.

Then let's say you put in parameters. Who has a weapon's license? So to get to him, my guess is for everybody who tells me, including in Congress, you should have found him, you're going to have at least 100 people who are going to Mike German and saying "Hey, I have a right to talk to whoever I want. I have a right to own a weapon." So what they don't consider is if you want to find that dude, who else is in the dragnet? And are we comfortable with you as a preventive organization taking the time to weed out the other 99 people? And they are really ticked off.

Shahid Buttar: Let me just say two things here. I think you're correctly identifying one of the process problems, which is that Congress has acted without ever considering the foreseeable consequences of the mandate, which is to say dramatic over inclusion. And the hypo, the diseased post, is actually not entirely hypothetical. Food Not Bombs is a domestic group from which participants have been deemed to commit more acts of eco terrorism than the baseline population. And Food Not Bombs chapters around the country have been essentially eviscerated by infiltration.

I mean, the same COINTELPRO tactic around disruption and sowing distrust, that's been happening in the environmental community for 15 years, even before 9/11. So I mean, whether or not it should be happening, it is happening. And I just want to again draw us back to the attention that we've not just talking about people with brown skin or people with a particular religious practice. This is a broadly applicable and felt problem that has impacted our civil society demonstrably.

Emily Berman: So my question looking forward now becomes a lot of what's been said is that there needs to be a closer look taken at various constitutional principles, Congress needs to pay more attention to what is actually happening in practice as a result of the attorney general guidelines. How do we get them to do that? Because I feel like we've seen this series of reports coming out of Glenn Fine's office that do nothing if not document

the fact that somebody needs to be paying closer attention to what's happening there. And it just gets no traction whatsoever.

Suzanne Spaulding: Part of the problem is the stovepipes in Congress. So you've got the judiciary committee, which has oversight over the Department of Justice and FBI, but they don't have all of the tickets for the classified – they don't have all of the entrée. I think they have the tickets, frankly, which is to say they have the clearances. They have staff with clearances. But they have a very hard time breaking through the secrecy barrier. You've got the Senate Intelligence Committee, which is like DNI, it's much more comfortable in the foreign intelligence realm than in the Homeland Security or Domestic Intelligence realm, and yet they're the ones who have the access to these intelligence-oriented programs.

And you've got the Homeland Security Committees, which think they too have an important piece of this. So I really do think – I think it's a challenge, and I think one of the things I've been pushing for, for years now and getting no traction so I don't know the answer to your traction issue, is that Congress needs to take a comprehensive look at this issue, and to do so, it needs to set up a task force, which the leadership of those key committees need to appoint members from their committee to sit on that task force.

And it needs to start by pressing the administration for a comprehensive threat assessment to look at the nature, scale, and scope of the threat because I think Matt Waxman is exactly right and others who have talked about this that the nature and scale and scope of the threat makes a big difference in terms of the kinds of tools and what you're going to do to address it. And then they need to look comprehensively at all of the tools we have for national security investigations and how have they been used and how are we using them and what have been the problems and what are potential problems in the future and how do we build in appropriate safe guards.

And I think that would help give the committee chairs, all of whom have a piece of this, a common operating picture.

Philip Mudd: Just a quick comment again. Something seriously that might be useful for an institution like this to look at. I always, in talking to security service friends around the world, was struck by how common the problem was we faced. We think of how different we are not only from Europe but from the Middle East when in terms of the threat, we're not. They're dealing increasingly with kids who are emotionally motivated, not ideologically motivated. We want to think they're different. They're not.

So what I'm suggesting is it might be an interesting project, which I haven't seen done, to look at countries in terms of technical surveillance and the constitutional and legal authority people have for technical and human source surveillance and security services and see how we're buffered. In other words, countries that are less intrusive, what is it that they do and don't do, and would we be comfortable moving in that direction? Most of the countries I dealt with looked at me and said you guys are nuts. They were more intrusive.

But my point is I'm not sure how difficult it would be simply to do a practical exercise to say you can go left or right, I don't mean politically, but less intrusive/more intrusive. And there are countries with experience in this in terms of constitution and law. What do you think?

Suzanne Spaulding: Although I do think you have to be really careful about those kinds of comparative studies, and I think it's worth doing. But I think, for example, we have imported a lot of thinking on this from the UK. And the UK was way out ahead of us in thinking about the domestic threat. Well, why? Because they have a far, far greater domestic threat than we do. It's on a totally different scale that the UK faces. And so you have to be careful, I think, and that's, again, why we always need to start with a realistic discussion about what is really the scale and the scope of the threat that we face here.

Emily Berman: I know Aziz and Shahid both want to follow up on that, and then I know we're out of time, but I'd like to take a couple of questions in the audience if people have them, if the panelists are willing to –

Aziz Huq: I want to make a very quick comment. So I'm more skeptical than I think Suzanne is in part about getting Congress's attention. And think about the incentive of an average Congressperson. You generally, in a first past the post win in the US, you win by 51 or 52, 55 percent, that's a very big victory. So you have very little incentive to do anything that is downside risky that could sharply dip your support and very little incentive to push your support much further up than it is. So you're much more worried about downside risk than you are upside risk. And that's a consequence of our first past the post system.

It's built into our politics. And as long as you have legislatures with that set of incentives, I wish it was otherwise, but I think it's very, very unlikely that you will get Congress stepping up to the plate in the way that Suzanne described. And just to be clear, it's built into our constitutional system.

Just to pick up on something that Phil said earlier but then also with your comparative comment. So two colleagues at NYU and I had been doing

assessment empirical research about taking large samples of the Muslim population in New York and in London and looking at the predicates of their behavior in response to the state. So we were able to draw judgments about or draw inferences about why do people cooperate, and that's principally what we're looking at.

But the one thing that we found that we've been able to do but we weren't expecting to do is that our data also allows us because we ask about attitudes toward political violence, we can also draw inferences about what predicts people's attitudes to political violence. And we're just starting to do that work and trying to figure out what the data tells us. But in trying to figure out where to situate our work in comparison to what's known, I was surprised at how not just thin, but almost non-existent the rigorous empirical work on that question is. There are lots of case studies.

And there has been I think actually appropriate caution about case studies expressed. There are lots of case studies. We actually know very, very little about what predicts people's attitudes toward political violence. And so just to give you an example of one of the things that we can look at that our data lets me look at is we ask people about violence and self-defense. Violence in taking revenge against somebody. We ask the people about political violence. Are those connected? So I think there is research going on which starts to guess at some of the question of what's the good proxy. And it's comparative in nature, and I think leverages some of the differences that Suzanne was talking about between different populations.

Shahid Buttar: And just to jump in on the question about Congress and how to change some of this and get to Suzanne's place around the recommendation, I think that in some respects, it's too easy to start with Congress or institutional actors. I mean, the battle we face is civilizational and cultural. We have to actually first shift the attitudes of the public, which is to say, around the questions of privacy, for instance, we have to build an awareness of the relevance to third party records as they relate to individual privacy. In a Facebook generation, I fear we have to simply get back to first principles in privacy. I mean, these values in the culture that inform the institutional calculus I fear are eroding.

And so to look at the institutions without considering movement building as a necessary pre-requisite to get to the point of meaningful interaction with the institutions, I think ignores a big part of the equation. And as we do that, I'd just say that we have around these principles like privacy and constitutional rights, a great many allies from very diverse political leanings. One of the raison d'être for the organization that I now lead was the introduction of the Patriot Act, which in very recent history has mobilized a very diverse, political constituencies, and you see people from both sides of the political spectrum expressing a very healthy and long

overdue, quite frankly, dose of skepticism with respect to the executive claims.

I think that leveraging those diverse constituencies that share abstract concerns, building a grassroots movement around it, which is another reason to look locally rather than Federally, and then over time, using that movement to, as movements have many times over American history, shift the tide in Washington is one of the things we have to be doing. I mean, no disdain for anyone in the room, but if I see another report, I think I'm going to shoot myself because we don't need reports. There have been enough reports. The IG has documented as many abuses as we – you all's reports are great.

All I mean to say is it takes more, and we're going to have to do some organizing. And we have to get out on the street, and we have to connect in communities.

Emily Berman: So I just learned that we all turn into pumpkins at 6:00 and need to be out of here, so let's take a couple of questions.

Elizabeth Goitein: I'll go quickly. I have just a very quick comment, and then a question. My comment was that I may have misunderstood you, Phil, but it almost seemed like you were saying that you have a choice between being preventive, which you're mandated to do and waiting until you have a factual predicate. And I guess I just wanted to comment that the idea of a factual predicate is not that wait until the bomb has gone off, but that you use the factual predicate that there may be a suspicion of criminal activity to try to them stop the crime before it happens.

But the question, and I hate to do this because I should give you a chance to respond but we can talk afterwards, but the main question I wanted to ask is I've read a couple of people recently who are saying we've lost the battle in terms of what kind of information is being collected, what sort of intelligence is being collected. The rules about how much we're pulling and what kind of information, that's done, and it's done in part because of the wealth of information that is held by third parties that Americans willingly give away. And it's in part because of the Facebook generation. If you don't value your privacy, then there's no need for the government to value it. I believe that. I think a reasonable expectation of privacy is what a person values. And if the next generation doesn't value their privacy, then that's fine. They get to decide that. So if that's where things are going, shouldn't we be talking, and I don't mean to suggest that I have an answer to this or that I believe one thing or another, but shouldn't the conversation be starting to focus a little more or a little less on what kinds of information are we getting and what the standard is and more on what are we doing with the information once we have it because the

government is going to get this information. What are the rules once they have it?

Philip Mudd: Just quickly, and that earlier point, we can talk about outside. But as both a security professional from CIA and the Bureau and as an American, I don't agree on your first premise. I think we should do both. I don't think that battle is lost. When I came across the Potomac River from the agency to the Bureau in 2005, I realized that we will never have a domestic intelligence service in this country. Intelligence is a pursuit of knowledge. What do we need to know about the Pakistani nuclear program? Lie, cheat, and steal, but get it because if they get nukes and Islamists take over, we got a problem. In this country, our first question is what is appropriate to pursue?

And I know this sounds Pollyannaish but boy, the world I saw at the Agency and the world I saw at the Bureau were fundamentally different. The Bureau makes mistakes. The IG has talked about it, the media has talked about it. But even in 2011, it's just night and day, so I don't think – I think both need to be looked at. I wouldn't, and maybe I'm a glass half full kind of guy, but I don't think the first piece from my optic is one I'd give up on.

Mike German: Phil, I was really intrigued with the idea of having civil society and the security agency switch sides, but I want to make it clear, I thought of that. I'm not kidding. We might have talked about that at DHS actually. I was nominated. Remember that? And I think you're exactly right in talking about the mandate of prevention and sort of the eternal vigilance that is felt in the agencies, which is what I think draws some of these views. But I found in working preventive counter terrorism as an undercover agent, using a criminal predicate, that actually helped me. So I think the question isn't should the FBI be focused on preventing but how should it be conducting that operation? And one of my big concerns is the false positive. As you said, you felt that if it was 100 percent hits, that meant you weren't trying hard enough.

So when we create a system that has a lowered standard and goes broader and starts collecting these false positives, not only are you violated the civil rights of the people involved potentially, but you're also creating a false alarm for every investigator out there doing those investigations. And I was really perplexed by your description of the Hassan case as an example because the FBI did, in fact, have an investigation of Hassan. So obviously, they met their standards. They did have wire tap surveillance that –

Philip Mudd: Not of Hassan.

Mike German: Not of Hassan, but uncovered multiple communications. Part of the problem was the agent doing the investigation didn't have access to a database that contained those, so but part of the problem is he spent four hours on the investigation. And I wonder if it's because he had done so many investigations where there was such a tenuous tie to any realistic threat that that actually made him less vigilant in actually conducting the investigation and whether we aren't creating a problem by expanding the number of false positives.

Philip Mudd: I hate to say it, it's like my comment about Andrea [Elliot], I think that one of the really interesting questions from the inside was we've talked almost entirely about how do you conduct an investigation, especially an investigation that's either predicated on behavioral activity or some broader indicator. We've got an organization in Britain that's not a terror organization but has been a funnel. What do you do? There's a flip side to this, and that is when do you provide specific policy guidance about dropping an investigation. Especially during my latter years at the Bureau, we worked more heavily on this because you found people wanted to kick stuff up to the headquarters before Hassan because they're afraid of a Hassan issue.

And for those who are not following me, what I'm saying is let's say you go up on surveillance technically or human source on somebody, and you drop it, and a year later, it does something. I understand a GS12, and that's roughly a major or something, a captain in the military who says now I'm leery about dropping that because if he pops up in a year or two, I'm in trouble. So what I'm saying as a long answer is focus on what policies and procedures you have to let somebody off the hook to say I'm not going to pursue this any further. That's a significant question. And the last, I'd say, is having sat at the threat table of the Bureau, the threat table of the Bureau is a fundamentally different than the threat table at the Agency because there's no threshold for strategic threat versus tactical threat.

Some 16-year-old in Topeka, you can't let him off the hook. But my point is the volume of threat I think if Americans saw sort of a reality show on the threat briefs we had every morning, they would be surprised. And some of it was what you said, sort of lower threshold stuff. You say dude, you got to let that case go. And some of it was just I don't know. I think the volume of second tier threat in this country would surprise most Americans. And that is not lower threshold stuff, and there's a lot of that stuff we should have dropped, but middle between serious and not serious. You're like "Man, I don't know what to do."

I'm not sure where we are in this one. But you're right, we should focus a lot on how you drop a case. We have too many cases running, I think.

Nusrat Choudhury: Hi. Nusrat Choudhury, also the ACLU, National Security Program. Thanks to all of you for your comments. And my question follows exactly the last two points that were made. What are the guidelines to stop an investigation? What are the guidelines in place right now to prevent the information that's collected either through this kind of third party lack of protection for privacy or through specific criminal investigations of certain people? What's used with the information, especially when the FBI is not only opening investigations but running the consolidated terrorism watch list, which has real impacts, and I think we haven't really talked about that issue, although it came up in numerous comments, it came up in a few other comments about what are the adverse impacts aside from chilling effects, aside from First Amendment rights and all of those things. People are being put on watch lists according to criteria that are secret in situations where redress is lacking.

And the ACLU has a suit addressing this issue challenging specifically the lack of redress in the no fly list, but this is certainly an issue with respect to other aspects of the watch list as well. So what I see here is a problem when we're talking about what are the lack of guidelines for opening up investigations, a lack of guidelines for what's happening to the information.

And there's a related problem of what's happening in the watch list context once this stuff gets into a database that right now, folks can't access a mechanism to get themselves off and to actually stand up for themselves. So there are three giant different problems in the room surrounding the issues that this panel has been talking about.

Philip Mudd: A quick comment. I think my colleague to the right mentioned this. I thought he was dead on. This phrase digital exhaust that is the 21st century, if you looked at a Dillinger case, how do you go after Dillinger? You find somebody who calls in and says this dude is a bad dude. I don't even know if we had telephone surveillance back then. But the access you have to follow someone is quite limited. You think of what you do every day, and you know this as well as I, with ATM's, I'm no Travelocity every day, with getting on Amazon. I think the question is a little bit broader than yours, and characterizing the question is simpler maybe than what you did, but solving it is more complicated.

And that is as we go into the 21st century, and people leave more and more digital exhaust, what are the American people represented by the Congress comfortable with in terms of Federal services trying to be preventive in looking at behaviors in that digital exhaust. I thought the guidance was – I think we need help on this because there's a lot we could do that we didn't. There's a lot foreign services did when we had [Rand] Beers**,** and

we said we could never do this. And I don't think people overseeing us understand both the capabilities we don't execute, how much danger there is down the road,and the volume of information someone leaves behind.

How you store that so if two years down the road, I open an investigation, and "Usha" was picked up two years ago. Well, should I have dumped that information or should I keep it in a secret vault so two years down the road, if her email address is picked up, I should know, shoot, we saw her two years before in Baltimore. The digital exhaust issue I think we're just on the cusp of and it is going to be huge.

Aziz Huq: And also, I think it's not correct to see it as solely as a national security issue. So think about the Federal prosecution going on now off Galleon Funds and the traders of Galleon Funds and the fact that if you're serious about enforcing even the securities laws that we have on the books now, which are maybe inadequate, the way in which government prosecutors and the DOJ will use aggregated information, financial information, will be – it is extraordinarily important to have access to that kind of information in other contexts. I think about the child pornography context and how do you go after people who are shipping trading –

Nusrat Choudhury: I think that makes sense, but I think my point was, which I probably didn't make very clearly, is that when you're opening up an investigation, the FBI is getting involved, that same entity is controlling the consolidated terrorism watch list, which right now doesn't have the adequate checks in the front end or the back end. So this conversation about what are the checks on the front end of opening up – conducting surveillance and opening up investigations – should also think about what are the longer term ramifications due to the lack of redress in the watch lists that are involved.

Phillip Mudd: I think you're probably right. I won't belabor this, and it may sound defensive, but when I was deputy director of Counter Terrorism and junk at CIA, I spent a disproportionate amount of time on watch list policy and procedure. And I think you're right on both ends, the front and the back end. I think the issue though was the low threshold for a mistake. To make this more difficult, it was about a national dialogue saying you know, if somebody might have sent money to a Hamas front three years ago, I got to tell you since I'm a private citizen now, I don't much care.

But the threshold is going to say that person is funding or providing funding through a front organization to a designated terrorist organization. I think we need to have a conversation about what risk we sit on as a free society, and I'm not trying to dodge your question. I'm trying to say the guidance we got was don't make a mistake. And so you're going to put

somebody who gave $20.00 to Hamas or to a front company in Detroit on the list.

Shahid Buttar: I just want to draw out a point of agreement because it sounds like you and Suzanne really –

Philip Mudd: What?

Shahid Buttar: I'll be quick. There's agreement here on the need to pay more attention to this question. What as a free society are we comfortable with in the digital realm? And the conversation we're having on this panel about human intelligence and investigations are very different than some of the concerns we were discussing in earlier panels around just intelligence collection generally and the databases. And I think there are common issues and also distinct issues, and I'm glad we had a chance to grapple with many of them.

Emily Berman: One more question.

Unidentified male: Do we still have an FBI that doesn't know how to do computers? I put the question because it's the same question that Sheldon Elson was cut off from giving this morning for lack of time. Now there's no time, but what's the status of it, and why can't they do it? Even I can do some of the stuff.

Philip Mudd: You're talking to a dude that doesn't have a TV, so let's be clear here as we go on, and I don't have computer access in my house. Let me go back to the law, and again, I was rereading the law this morning. Boy what a horrible life the private sector is reading the Intelligence Reform Act at 7:30 in the morning – that's your fault, Emily, by the way. It does talk about not only things like developing a preventive capability and training, but it talks about sort of bringing the Bureau on par with the rest of the intelligence community. Let me make a sort of broad comment about budgetary process and information technology in the 21st century.

The Bureau is not close to on par with the intelligence community. I'm not talking about access to records and stuff, just in terms of IT, they're not. My perception is that still in this government, we view investment in IT in sort of 20th century terms. Do you need this system? Do you need that system? How do you become on par with the intelligence community? And this is a personal perspective, but my view is the government has to get to a point as the private sector is about understanding that every year, you need reinvestment in IT. It is not an episodic investment, and it is billions and tens of billions.

And because the Bureau has started behind the curve with the intelligence community, they're still behind the curve. And until we have an acknowledgment of how much money you got to spend every year as a recurring investment. It is not a 2010 investment in a new system to make the Bureau compliant with top-secret regulations. It is 2010, 2011, and I don't see that. So yes, they are behind.

Emily Berman: On that optimistic note, I'd like to thank everyone for being here, and I think Faiza wants to say a few closing words.

Faiza Patel: So it seems that I'm the bad guy. I always have to tell everybody it's time to go. But I just wanted to thank Atlantic for hosting us today, which has been great and to thank our panelists, and to especially thank all of those who stuck it out until the bitter end, but I think it's been a really stimulating discussion. And we look forward to continuing the conversation. Thank you.