PANEL DISCUSSION:

"NO PLACE TO HIDE: WHERE THE DATA REVOLUTION MEETS HOMELAND SECURITY"

MODERATOR:

P. J. CROWLEY,
SENIOR FELLOW,
CENTER FOR AMERICAN PROGRESS

FEATURING:

GENERAL WESLEY K. CLARK

JAMES X. DEMPSEY,
EXECUTIVE DIRECTOR,
CENTER FOR DEMOCRACY AND TECHNOLOGY

NUALA O'CONNOR KELLY,
CHIEF PRIVACY OFFICER,
DEPARTMENT OF HOMELAND SECURITY

ROBERT O'HARROW, JR.,
REPORTER, *WASHINGTON POST*;
AUTHOR, *NO PLACE TO HIDE*

9:30 A.M. – 11:30 A.M.
WEDNESDAY, MAY 4, 2005

Transcript provided by
DC Transcription & Media Repurposing

P.J. CROWLEY: I am P. J. Crowley. I am a senior fellow here at the Center for American Progress. We welcome you all here today for a very important, complex, vast issue of significance to our country and our society. I want to welcome my fellow panelists here. I think this is a terrific program and we appreciate all of you coming to it.

Perhaps the greatest post-9/11 challenge we face is deciding how to achieve better security; how to protect our free and open society without fundamentally altering how we live, how we are governed, what we represent as the people and how we relate to the rest of the world. We have yet to determine how to balance security and privacy if balance is in fact the right word. What is possible? What risks do we simply have to live with? What impact government is permitted to have in our personal lives and what does it mean for our right to privacy?

Security is only one force shaping our world, technology is another. We viewed these as distinct things before 9/11. As Robert O'Harrow will tell us, the two have clearly intersected since 9/11. We have assembled a distinguished panel here today to help us understand the implications.

We continue to confront a clear and present threat here in United States from global extremists. You know, contrary to what the administration suggests, they have not all gone to Iraq. They are still here and they still pose a significant threat to us. We have made what they want to do – plan and execute another spectacular attack against an iconic structure in urban area involving a large number of civilians, we have made such an attack clearly harder to accomplish but not impossible.

We have fixed a lot of what went wrong on September 11. We see changes at airports, government buildings, and borders. However, there are still significant gaps primarily because the problem is so vast and new and partly because the resources devoted to the tasks are not yet sufficient. As the 9/11 Commission said, broad elements of our government then were not in the national security business. The Department of Homeland Security is aimed at correcting this. Regardless of how our government is structured, the key is better intelligence. Better intelligence requires both better information and the means to effectively analyze that data so we can, in the 9/11 vernacular, connect the dots and deter future attacks.

We have a new director of national intelligence and a national counterterrorism center. We did not pursue a British style MI5 Domestic Intelligence Service in large part because many – to many would go beyond our tradition of limited government. Nonetheless, as law enforcement seeks more and better information, most of which resides in the public – in the private domain, what burden do we place on the law-abiding citizens we are charged to protect? Everyone has great faith that technology is a major part of the solution. Thomas Friedman in his latest book, *The World is Flat*, discusses

how technology has enabled unparallel private sector collaboration and leveled the global playing field. He acknowledges the dark side of this phenomenon and that technology has empowered individuals of like thinking to do good and evil.

Robert O'Harrow focuses on the flip side of this coin. In *No Place to Hide* he shows that given the prospect of evil how the private and public sectors are adapting to our country's security needs unquestionably in ways that make us safer, without a potential cost to our society. He rightly points out in his book that technology is advancing far more rapidly than its policy framework. He also questions whether the American people really understand how this is evolving and how much information is now accessible to the government either directly or through third parties.

The 9/11 commission broached the prospect that at some point, U.S. citizens and U.S. persons would be required to prove who they are – who they say they are and have a right to be where they are. We are only beginning to this vital debate regarding, how, when, and by whom this should be done and to whom this should apply. The real ID debate or lack of a debate is a lost opportunity. Unfortunately, the legislation under consideration the Congress right now has not really been debated at all. Most people understand the link between security and travel, given how 9/11 unfolded. Most people understand the need for greater security around our critical infrastructure and essential operations of government. There is far less agreement as to the appropriate means of identification and verification: a de facto national ID like the driver's license or an actual national ID. There has been even less public discussion regarding the kinds of information, databases, protocols, and legal protections that would be required to support any kind of smart credential.

We have yet to find our Goldilocks point, if that's what you want to call it, regarding security and privacy. The Total Information Awareness program, later renamed the Terrorist Information Awareness program; CAPPS II; the revised airline passenger screening system that failed because the government overreached by extending the program's application beyond its security and terrorism mandate; the incident involving Jet Blue. We have yet to get it just right with the mix of data collection and analysis and privacy protections and oversight.

What is clear is the American people need to be more engaged and understand the promise of technology and its potential risks. To borrow a Rumsfeldian phrase, homeland security can't be an unknown known, where the American people do not understand how the government is acting on its behalf, but potentially at its expense. Homeland security will be sustainable over time only if it has the clear consent and involvement of the American people.

We at the Center for American Progress are trying to enhance this debate, not only through this forum and others that we will conduct in the upcoming months, but also in your chairs we have a paper written by my colleague Reece Rushing that begins to lay out some preliminary observations and recommendations on this issue, principally aimed at recommending that we update the Privacy Act of 1974; it's 30 years old. I remember

when that changed our lives in the military, and clearly it was designed for a different time, a different age, and has not necessarily been geared to the technology and promise that we see.

So thank you very much. We are very pleased to have our colleagues here today. I will briefly introduce them, but in your packets there are extensive biographies. It's a impressive group, all of whom have been focused on this issue for quite some time. To my far right, Robert O'Harrow, a reporter for the *Washington Post* and author of this book, *No Place To Hide*, and magically as you – if you are intrigued by this discussion today, magically as you leave, their will be the opportunity to purchase this book if you haven't already.

To my right, General Wesley K. Clark – extensive biography; a man – a four-star general who I had the pleasure of working with for a number of years in and around the Pentagon has since done a number of things including running for president. Anyone here from Oklahoma?

MS. : (Off mike.)

MR. CROWLEY: Okay then.

And to my left, James X. Dempsey is executive director of the Center for Democracy and Technology. He has a few prominent places in Robert O'Harrow's book. And to my immediate left, Nuala O'Connor Kelly, who is the chief privacy officer for the Department of Homeland Security; and as you will see in our paper and through our discussion, it's kind of a model in many respects of how we think the issue of privacy needs to evolve across the government as we tackle this very difficult issue.

What we are going to do here since we are highlighting first of all the book, we'll let Robert O'Harrow kind of set the agenda – you know, establish the framework for the discussion this morning. We will kick the issue around with our panelists for a little bit before opening up the balance of time for questions. As Theo comes around during the course of the discussion, by all means introduce yourselves, tell us who you are, who you represent. If there are working press here this morning, we will invite them to ask the first questions when we open the floor.

We here at the Center For American Progress do not support the nuclear option; however, as the moderator I will definitely use it as necessary. We want to keep this as a dynamic discussion, but we will limit debate from the floor, if you will. Please, if you are called upon, as Alex Trebek would say, you know, form your remarks in the form of a question.

With that we will let Robert O'Harrow begin.

ROBERT O'HARROW: I am not sure if there is anything left to say. That was a marvelous overview of the issues, so maybe I should just remain silent here. (Laughter.)

A little background, and this is all stuff that's going to be familiar and hopefully it will build to a point. In the 1990s I think we can all – many of us anyway – think back to when we had computers with orange screens back in the early 1990s or late '80s. And they did a lot of things, but they are almost neanderthal now in retrospect. And starting with those PCs that we all had, there was an explosion in computing power that we are also realizing now on desktop. It's amazing what can happen on your PCs. Well, in a parallel way the private sector saw an explosion in computing power and a remarkable drop in the cost of data storage and then of course the expansion of the internet and other types of networks so that those phenomena enabled a data revolution and enabled private companies to collect more mundane details about us and about everything than ever before.

At the same time, we saw a really fascinating shift in the philosophy of marketing. Marketers realized that with enough information they could start trying to treat people in a million at a time as individuals and they could treat – let's see, what's happening here – they could treat people a million at a time as individuals and try to market them one to one, so that if you had a particular type or cut of jeans, if you had a particular predilection for certain types of books, sweaters, the list goes on and on – they figured as if they could build enough information about you and your income and the kind of car you drove, and house you own, and the neighborhood you lived in, the sweaters you bought, the books you read, the magazines that you subscribe to and on and on and on, that with help from statisticians and people who do such things as psychographic modeling they could get better and better at marketing. And in fact they have. For all the flaws and the mis-sent mail, which still suggests what their early stages of all this, they have got much, much better at targeting you for marketing, and we like that in many cases. We like that sort of one-to-one service. And so as a consequence many of us fuel this one-to-one marketing revolution. We fill out surveys, we fill out warranty cards; and information like that, coupled with publicly available records, coupled with our purchases has helped to provide us the benefits that we like so much and at the same time to help in a sense provide rocket fuel to this data revolution.

Now, a lot of that had to do with marketing and the private sector and there were question, no doubt, about what we at the time in '90s called privacy. The notion that a private companies could have unlisted phone numbers that we paid to have unlisted – many people found that unsettling.

There was a company, as many of you might recall, they was buying up driver's license images – the photos – to create an anti-fraud system they said, and that blew a lot of peoples minds and created all sorts of firestorms. The list of so-called privacy intrusions or debates went on and on. There was a company that was buying up prescription records you might recall. It was called the Alensis (sp) and it was buying prescription records from pharmacies around the country, and during something that was a real social good or striving to do something that was a social good, which was called drug compliance. It was going to – this company was going to remind people to take their medicine. What they didn't tell people, of course, is that they were also working with drug companies to send out educational materials about particular drugs to people

with particular ailments. People went wild when they heard that because medical privacy trumps even our financial privacy.

Now, all of this was going on sort of as an open secret, although few of us really understood what was happening behind the scenes and partly that was because we didn't bother to ask and partly it was because the companies themselves knew – and we know this from internal documents, we know this from SEC filings, we know this from lots of interviews – they didn't want to really tell us what they are doing because they were afraid – guess what? – it would make us very unhappy and it went unsettle us because we wanted the benefits, but we didn't really want to know how the sausage was being made.

Now, that's the scene. That's the context. Then comes one of the most horrendous things in American history: 9/11. And lot of these same companies that had all these information out of very earnest impulses flung open their data systems and said "We don't know if there is other terrorists out their in our midst. Here is our data. You can find these links. We can find out every place that they lived, all the people they had contact with. Use our data." And we are talking about everyone from grocery store data collectors to banks to the credit issuers to large data marketers, LexisNexis, Choice Point, Axiom, some of the names that you are probably starting to become familiar with.

And it was an amazing thing and to my mind it's still a dazzling phenomenon; not only the data revolution, but this impulse to help right after 9/11 – there is a fellow, Michel Jackson, who is number two at Homeland now, as he pointed out to me, quickly merged – the patriotic impulse quickly merged with the profit impulse. They realized that out of this tectonic shift that was 9/11 was going to grow a tremendous financial opportunity. It was going to be a gold rush, so that you would have possibilities of serving as a contractor on the war on terror to protect homeland security, and so that patriotic impulse very quickly turned to shaping business plans around providing security. And if you think that's inherently wrong, I would argue to the end of the day that it is not inherently wrong; that this is what business – businesses are in business to make profits and that is not necessarily a bad thing.

What I see coming out of this that's troubling, however, is that all this or very much of it was going on in secret. And there was a fellow named Peter Swier who was Clinton's privacies czar – the first privacy counselor in the government, and he pointed out that what we saw happening was the beginning of a security industrial complex and the reason that mattered is that it echoed something that Eisenhower had said in 1961 when he was leaving the government, I am going to read you a little passage because I just find it remarkable how applicable these words are to us today.

When he was leaving the White House, President Eisenhower said, "In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex. The potential for the disastrous rise of misplaced power exists and will persist," Eisenhower said, "We must never let the way of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel

the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals so that security and liberty may prosper together." I think that is amazing. Switch the words "military industrial" to "security industrial" and you have something that I think is perfectly applicable at an early stage.

And the reason that I am convinced that lot of this is going on in secret is that I worked very hard for two years to find out what some of these projects – what was happening, who was lobbying whom, who was making money of this, what kind data was being used and so I dealt with people from a lot of these companies – Axiom, LexisNexis, Choice Point – and when you knocked on their doors the very first thing they said and the thing they said as often as I asked, maybe hundreds of times – I can absorb a lot of pain – was "No, that's not – we don't have the right to tell you that. We are not allowed to tell you that. Go to the government." And so I would go to the government in these agencies and after, in some cases, getting through the vanguard of public affairs officials who said "No, no, no, no," I would then get to someone who knew and they would say "We can't talk about it."

So that is – to my way of thinking, the label "security sensitive" just didn't cut it. A lot of this stuff was not going to be – it wasn't going to undermine – CAPPS would not be undermined and was not undermined by exposure or by the exposure of secrets. National security wasn't undermined, in part because we took care not to reveal secrets that might undermine the secret codes they were using to profile people. And likewise with Total Information Awareness, it was possible to talk about that and move the ball way forward without giving away secrets to the terrorists, who in fact did want to know how these things were working. But just because they want to know doesn't mean we can't know. There is a balance that we can strike in terms of an open public debate about this.

There is a guy that I think many of us in the room respect and admire deeply, General Clark, and he serves as a great example of someone who was deeply involved in representing a company called Axiom. And Axiom was one of those companies that responded with – I know that from my reporting – very patriotic motives. They had a lot of that as a marketer and they shared it and they shared it to good effect; it helped. They also saw ways that they could change their business model and become part of the security industrial complex. And one of the people that was helping open doors for Axiom in Washington was General Clark. The reason I raise that is because I kept finding the General Clark got to places before I did and people spoke admiringly of his ability to say what he knew, to say what he didn't know, to play it straight, and to in every case do it in the smart way, which is why people respect him.

The thing that triggered or bothered me is that when I asked Axiom to talk to General Clark, he couldn't do. When I asked General Clark's people to talk about what he was doing or what Axiom was doing – couldn't do it. And it is the sign that even people we respect sometimes aren't accessible to tell us about how the world is changing in a pre fundamental way, and so my thinking is, as a reporter, is that even the good guys

shouldn't get a pass in the post 9/11 era. Everybody should be held to account for what we're doing.

So I am going to cut it off there and I guess I want to read one little passage before I pass the baton because I think it's interesting and it puts this in, to my mind, a slightly different historical context. And it's about five paragraphs.

> On March 15th, 2002, at a coliseum in Fayetteville, North Carolina, President George W. Bush beamed as the soldiers from Fort Bragg and their families chanted: "U.S.A.! U.S.A.! U.S.A.!" The memories of the attacks six months before were fresh. The president was there to spell out his plans for a long, relentless war on terror. "We want every terrorist to be made to live like an international fugitive: on the road, with no place to settle, no place to organize, no place to hide." It was a powerful moment.
>
> It also was an ironic echo to a warning from Senator Frank Church three decades before. Church had served as head of a commission formed to examine the nation's history of domestic surveillance. He had seen firsthand what could happen when law enforcement and intelligence agencies amass too much secret influence. In the late 1960s and early '70s, some worked outside the rules, targeting innocent people and groups for their political views or because someone mistakenly assumed an individual posed a threat.
>
> Church was especially concerned about the government's use of computers and eavesdropping technology. Such equipment, he said, could serve as a powerful weapon abroad, but the use of it could also spin out of control, especially in the hands of tyrannical leaders. And then he said "That capability at any time could be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter," he said on a television news program in 1975. "There would be no place to hide."
>
> Like it or not, the technology is now being turned on American citizens and foreigners alike. It is being deployed at every level of law enforcement and intelligence. It's vastly more powerful, varied, and sophisticated than Church ever imagined those many years ago. As a consequence, the president's wish may come true, and the terrorist will have no place to hide. But then, there's a chance that neither will we.

MR. CROWLEY: Robert, thank you very much. Obviously with that framework I want to give each of the panelist an opportunity to respond to the framework that Robert has outlined for us, provide their own opening comments, general and particular. You obviously moving from your military career into your business career, saw something very important and in this issue – what Axiom was trying to do. If you would, as part of your remarks, describe what you would consider – you know, what are the security imperatives that you see here? Clearly, as we will see, there is absolute tension and

probably a healthy tension between our security interest, our privacy interest – how you, in essence, balance those two.

WESLEY CLARK: Well, thanks. First of all, I have read parts of this book and I followed all of Robert's work in the *Post*. I think it's good work and I am a strong believer in the fourth estate and public scrutiny and – you know, I grow up like most of this did in the '60s on Eisenhower's statement about the military industrial complex, but we are in the very early stages of looking at data and security.

I respect Senator Church and what he said in 1975 and it was visionary and the results of it were that the U.S. military was barred from collecting information on U.S. citizens. It was so bad at one point that as a battalion S-3, I couldn't get the telephone numbers of the people that worked for me because they said, "Sir, this is protected by privacy," and, you know, when you tell the military to do something, we do it and we do really well. So we really guarded each other's phone numbers from each other, and I don't mean to make fun of it. I mean if this is a legitimate concern; we just have to get the balance right.

I think if you look at where we are, as Robert said, we've got tremendously enhanced capacities in some areas. We can certainly monitor telephone calls. We can certainly monitor financial transactions. We can probably – someone can probably monitor financial transactions in real time. I think First Data does that, but of course they don't know everything about the transaction. There are video cameras out and there are companies selling systems that can monitor hundreds of video cameras and there is facial recognition technology where presumably with the right kind mathematical mapping you can take a side snapshot of someone, rotate, lock it in, figure out who they are, and then roll up their life history and these cameras can be deployed on streets. They could be at the street corner. They could look at your car, get your license plate, and run a – you know, you are already walking through that every day. Every building you walk into has a security camera. Most of those security cameras are connected to something, you don't know what, and most of them record information and you don't know where it goes. So the thing that's not quite done yet is all of that information is not quite assembled, but it is all out there. So this is very appropriate to discussion.

From the security angle of trying to use this data, you need to know two things. First, we really need to know who is around us. If we lived in a small village, we would know that. In Concorde, Massachusetts's, pre-Revolutionary War, people knew each other. And when someone rode through and they were stranger, they were recognized. In America today, people don't know that. So this concept is the genesis of the so-called Trusted Traveler program where if you just knew who people were – you know, you don't know them because you can't really know them, but you know about the. You know they're real people and that they have families, that (they're schooled?), that they're American citizens, that they've got a job, whatever. There are not people who are going to cause a problem. They're not a security threat. So you would like to know who people are.

The other thing is what you'd hypothetically like to know is if someone, either known or unknown, is undertaking a pattern of events which might prove threatening and the Secret Service always does this. If there is threat to the president, the Secret Service is there. They investigate people who threaten the nation's leadership. And the question is: how does data play into this? So we already have a program that does data – CAPPS I. If you ever got searched going on an airplane, you wondered how you got the so-called random search or it's marked SSS on the ticket and there are algorithms. For example, the people who wrote this believed that terrorists probably would have to pay in cash, so if you buy ticket in cash, you are going to get searched. Or that a terrorist would try to fake us out by switching flights at the last minute to throw off pursuit, so if you've ever had a last-minute change of plans, then you might get searched. Or that you – a terrorist might only fly in one direction, so if you have a one-way ticket you might get searched. You've come up under these algorithms and they're very crude and rudimentary.

What we have to do is get the right balance in the society from using the – to use the data to protect us, but not to take away our privacy and we have to move through this process of making people aware of the data. You cannot escape this data. This is – you cannot turn back the clock, I don't think, on the data. You can't rid of checking accounts, television, recorders – I mean, cell phones: they here to stay. Most of them now don't have GPS coordinates in them, but some of them do and in a couple of years they'll all have GPS coordinates so you'll know exactly where the person is calling from if you have access to that algorithm. It is going go on and on, so we have to get comfortable with it. We have to set some boundaries and some rules on how to project our privacy and use it to protect our country, so it's the matter of tradeoffs.

We have been through this before in American society. You know, the progressive movement got its start with meat packing industry. When we started in America, you raised your own cattle and you butchered your own cattle and you spun the chicken around and cleaned it, plucked the chicken I mean, like we did at Ranger school. (Laughter.) But we don't do that anymore. We go butchers. We have the Food and Drug Admin. We inspect meat plants and we have trust in that. Of course, we are worried because there is a potential security threat, but most of us still eat hotdogs, which is an astonishing thing. (Laughter.)

And in the 1920's by the time it got to where taxi cab drivers were telling you what stocks to buy, people began to say the stock market is in trouble, and of course it did collapse and a whole new network of regulations were put in place. National Association Security Dealers came in and they licensed people that sell securities and it's backed up by the Securities and Exchange Commission and legal penalties. Systems like this have to emerge to protect our privacy and get the balance right between our need for privacy and our need for security and the public's needs for security. And it involves some combination of regulatory authority, citizens groups, watchdog groups, challenges in court, and industry associations. And so I think this forum today is a good chance to talk about those issues, P. J., and raise them and get it all out there.

Can I just say one more thing about this impulse to privacy that you've mentioned, Bob, because when I was doing this – and I want to say this because Nuala is here, because when the government starts working programs and it does know where they go and where they going they are always cautious because everybody knows that these programs that do data are very sensitive. Before the government could even get a grip on some of these programs, when the word comes out on them they are blasted before people even understand it. So on the one hand, I understand exactly why there is an impulse for privacy. People – companies like Axiom were told, "Look, you just can't compete for this contract if you talk about this to the press because we don't know what the program is and we want to have – we want to be able to –" this is – I'm speaking for the government – "We want to be able to see what data you have available. We want to figure out if we can use it, and we don't want to have to answer a million enquiries from the press about it until we get it done. Then we'll run it through."

You know, my instinct on it was a little bit different than the government's, but I didn't have any influence on them. I mean, my instinct would have to bring in the ACLU and to say, "Please create a group that's sort of like a trusted group that we can bounce ideas off of and we want to run these ideas by you. And if you have strong objections, we want to hear them. We want to hear them right upfront. What we ask is that you will work with us in a collaborative sense so that – you know, you tell us before you run out to the *Washington Post* the next day and we have got (unintelligible.)" So, you know, we are just exploring ideas. We want to try to put this together and I do think there is a need for that. There is a need for enough privacy in governmental decision-making that the government can come out with programs and then have a chance to explain them, not to take anything away from the press because that balance is a dynamic balance. It's fought by and maintained by hardworking reporters who make a lot of phone calls and get turned down a lot, but it's a very important public duty.

So I am not sure if the balance is right is what I am saying. I don't know if it's right and that is one of issues we ought to explore.

MR. CROWLEY: Thank you, General.

Probably if – in Robert O'Harrow's speed-dial somewhere there is Jim Dempsey, who is perhaps one of the blasters when these issues come up. You know, Jim obviously – you know, the general has outlined some of the clearly – you know, security imperatives here. In your view, correspondingly, what are the privacy imperatives? What are the implications? We are obviously moving beyond the domain that the Privacy Act anticipated. You know, that was geared towards public databases; we are now moving to a system that will be dominated probably by private databases. What are the some of the implications?

JAMES DEMPSEY: Well, I think you referred, P. J., in your comments to attention between privacy and security, although reading Robert's book and listening to some of the comments of General Clark one could be reminded of Scott McNally, the chairman or CEO of a major tech company who said, "You have no privacy. Get over

it." I actually don't see this issue so much either as attention that is privacy versus security. I think post-9/11 one of the worst metaphors we have had is that sort of dichotomous metaphor that almost suggests that there's like a mathematical formula; that if you give up some privacy or some civil liberties, you will purchase some security in response. And I think that is the wrong way to look at privacy.

Privacy, remember, is not so much, here – when we are talking about information privacy, it is not so much about what is secret, but it is about how information is used and about we what we would call fair information practices about accountability and transparency redress. For a long time I think some privacy advocates took comfort in government inefficiency – that because the government was inefficient we were better off from a civil liberties standpoint. And I think that is clearly no longer true. As the general said, the technology has far surpassed that to the extent that you can no longer rely upon sort of what the Supreme Court once referred as the practical obscurity of data to protect your privacy; that what had once been practically obscure is now widely collected and shared. So we have to look to a web of protections; this whole system of checks and balances, transparency, accountability, redress.

General Clark referred to the sort of small town and this sort of – you know, there is always a debate over this sort of a metaphor and we are trying to get back to this small town where everybody knew each other. You know, this small town – a lot of people hated it, of course, which is why they moved to the big city. (Laughter.) But also the small town had its checks and balances: you knew everything about me, but I knew everything about you. Two years ago people even didn't know the name Axiom. Axiom knew everything about me. I knew about them, but most people didn't. So we did not have a small town; we had a disequilibrium there and I think a little bit what were talking about here– if we are about taking creating these – you know, the small town – you know the busybody could be sanctioned in various ways, and I think what we have got to figure out is how do we create that for this new environment and not trying to roll back the tide of technology; clearly that is not going happen.

I think one of the points of Robert's book is – and I remember a quote in an FBI budget request – I was one of the few people who actually read FBI budget requests outside of OMB or the FBI and they are good documents because of course they always more money so they are going to tell you things in the budget proposal that they won't tell you otherwise. And they were asking for more money for processing of intercepted communications and pointed out in there that the drive of technology alone – consumer-driven changes in technology would be putting more information in the hands of the hands of the government, making more information available to the government separate and apart from any government mandate, any governmental push; just the consumer-driven demands. And GPS is a perfect example. People like it because it is convenient. Robert talks about the benefits of these and we don't – nobody, I think, is trying to turn back those benefits, so instead how do we create this web of protections?

One point that I think needs some significant line drawing – all of these lines are kind of spectrum of course, but I think we can draw distinction between the sort of use of

commercial data – by the way, here we are talking primarily I think about commercial data and the sort of – we are not talking about what the government can do with the data that the government collects for law enforcement and intelligence purposes. There is a huge set of very difficult and serious issues there. But the commercial data, I think, on a – is useful for locating people, for finding out more about people, for building a case through the sort of traditional building blocks of investigative practice (and just?) sort of predicated. You've got some nugget of information and you are trying to track it down. You've a name; you are trying to find an address. You've got a partial license plate number; you are trying to find a child abductor.

I think where a lot of the debate has gotten off track, and Nuala's boss stumbled just the other day on this talking about red – taking lots of data and red-flagging people and the general somewhat slipped over into this. I just think that the predictive capability for counterterrorism purposes of commercial data and of current analytic capabilities is grossly hyped and exaggerated. I just don't think it's there. Now, I think that the defunding of TIA or the moving of TIA into more the black side of the budget was a mistake. I actually think that the research on TIA should have gone forward, but to me there is a fundamental difference between saying "Based upon millions of book purchases, if you bought this book, you may like this book." Really all we are saying there is, other people who bought the book you are buying also bought this book and we just know that – I mean, people's reading habits obviously fall into patterns.

Or even in the fraud detection area looking at millions and millions of credit applications and tracing them over there lifetime and some go bad – a certain percentage are fraudulent applications. People are applying for credit not intending to pay the bills, okay. Millions and millions of those can be analyzed, so that then when the next application comes in you can say, "This one may be fraudulent." We will give it a score that says this is more likely to be a fraudulent application than a legitimate application based upon millions of these that we have looked at. It's very, very different to say this applicant for credit is going to be a child molester. I just don't think we have that capability to look at millions and millions of credit applications and pick out the child molester, and I don't think that we can pick out the terrorist either. And I think some of the hype that is come forward here – and some of this – what's the term, Robert? – industrial military surveillance of –

MR. O'HARROW: Security industrial complex.

MR. DEMPSEY: Okay. I think that – you know, a little bit of a provocative term, but I do think that there has been this kind of hype around this predictive capability and the leap from the kind of marketing applications or fraud detection applications that are used to the – we can find out of this ocean of data the likely terrorist, particularly given the fact that – what? – the FBI has how many hundreds of thousands of hours of untranslated FISA taps? The notion that we are still not using information that was collected on a predicated basis that the information that we have generated from Guantanamo, from our liaison relationships with other governments, all of this information that provides these tips and leads, using the commercial data to flush that out

and to try to say is this guy in the United States or not, like al Midhar and Hasmi were, I think that's legitimate, but to try to think that we are going to able to make that predictive capability, I think that's a leap. At the very least, it's at the research phase, not at the implementation phase.

And I think that though I am – I was shocked to see this – I don't know if you saw this report. It didn't get widely covered, but Secretary Chertoff mused the other day – and it was musing, but he mused the other day that it would be possible to sort of collect all this data. He proposed putting it with a nonprofit entity, which destroys all the accountability aspects, too. (Laughter.) Not that nonprofits are unaccountable, no. But they're just not – the Privacy Act doesn't apply to them. Here we are talking about how to create a structure of accountability here.

So anyhow, I think the General Clark was a 100 percent correct that Robert's book – you know, Robert's book I think has not a single policy recommendation in it, which is a tribute to Robert as a journalist. (Laughter.)

MR. CROWLEY: Maybe unusual for the *Washington Post*, however. (Laughter.)

MR. DEMPSEY: Well, yeah.

MR. O'HARROW: It's called the easy out.

MR. DEMPSEY: Well, it's partly – it's also called the honest way or at least the honest journalist way; not a single policy prescription in that book. Now it is time to begin to develop that policy framework.

MR. CROWLEY: Which is a marvelous segue to our last panelist. You are the person in the middle, obviously, to try to you know do both. I noted your job descriptions says that your task is to assure that the use of technologies sustain and do not erode privacy protection relating to the use, collection, and disclosure of personal information – piece of cake.

NUALA O'CONNOR KELLY: Well, thank you for that introduction, and it was a great segue from Jim. I am honored to be on a panel of such distinguished thinkers about this issue and I am grateful that not only they, but all of you are here to talk about this because personally I think this is really one of the most compelling public policy issues facing our country today.

I want to start with just a little comment on something Robert said and it was just an offhand comment about the orange screen. There are a couple of people in this room that smirked who were obviously too young to remember the orange screen and I saw them. I am not going to point them out, but that to me says that we each are coming at this issues of technology and privacy from an incredibly different perspective, whether it's generational, societal, cultural. And the challenge, I think, for our government is to

think about ways that respect those differences, that allow us the greatest amount of autonomy and personal privacy, while also creating a platform of security. And if I can just talk a little about my job and really where I am coming from before we go to questions, my job all day long is to worry about personal privacy. Others at the Department of Homeland Security worry about borders, they worry about airports, they worry about all these other things. I worry about how this department impacts your life, your personal privacy, the data of visitors to this country, and of those who would seek immigrations status or other status.

We do that formally and informally through enforcing the Privacy Act, so I am very excited to read that paper that was mentioned and I think there are incredible opportunities here to think about how our laws have and have not kept up with technology. We also enforce a privacy impact assessment program which requires every program to articulate the very questions that we're talking about: how it is impacting individual privacy, what data has been collected, what private sector partners are being used?

We actually also oversee the Freedom of Information Act, which I think it's an interesting corollary. We want to keep private your personal data, but we also want to make transparent and accountable what this agency is doing in terms of new programs, in terms of new policies. I think that it was a construct actually that was articulated to me by one of Jim's colleagues, and I have to give Ari Schwartz credit, that in an environment where some of our activities are necessarily not transparent or not opaque because of necessary, ongoing law enforcement or counterterrorism activity, the mindset – the process of thinking – the process of policy development has to be that much more transparent to get the accountability, to get the public (into our?) commentary, to get the public response to those programs, just as the general suggested. I think that that's exactly what my office does every day; both formally and informally reach out to the public, try to hear the complaints, the criticisms, the concerns, as well as the positives.

How did I get here? I started in the government just a days before 9/11, actually, and unlike those in the private sector who had the – what was it? – the profit motive as well as the motive to help, my motive was I have done this before. I had started a privacy department in private sector. I knew that this was going to be a compelling issue for this agency, which combined 22 former separate agencies and created a handful of new ones, which meant that there was data of all sorts and all types across these agencies that could potentially be commingled and that this was an agency that needed a privacy framework. And so I am grateful for the comment that we have served as a model for other agencies. I do believe we have. We are first of our kind. We are the first statutorily required privacy office.

But I should also say, personally I come with – I don't want to call it baggage, but some personal interest in this issue. I nearly lost a sibling on 9/11. I had a brother-in-law in the World Trade Center who was injured and so my family was personally affected. I have nieces and nephews who might have lost their parent in that event. But I also was born and raised partly in Northern Ireland and I saw the impact of government intrusion

and government surveillance on the individual in a way that can be incredibly debilitating to the individual when carried out ineffectively or inappropriately and so there are – there are two sides to this coin, but I would not say they are balancing.

Let me encourage everyone to strike the word balance from his or her vocabulary. We are talking about privacy and national security. It is not an either/or and there are number of reasons why I say that. First, in times of crisis, if you are talking about privacy versus security, privacy is going to lose and that is not okay. My job and your interest in privacy are not mutable forces that can rise and fall depending on our level of crisis and our concern. They are immutable. They may be different among each of you, but they are your right, your value, your value to this country. So I would say there are consonant structures, as Jim mentioned: the fair information principles, values, respect for the individual and the Privacy Act and FOIA and other legal constructs that should remain immutable, whether in times of crisis or not.

I would say – and my flippant response to the balancing comment is, try being the chief privacy officer at Homeland Security and raising a one-year-old; now that's balancing because there is a limited amount of hours in the day and it is not an easy job. All working moms and all stay-at-homes moms know the balance of getting everything done in the day. These are two – privacy and security are two important, compelling, fundamental public policy interests, goals for our government to achieve. They can be achieved together.

One of the quotes that Bob mentioned from Eisenhower was that security and liberty may prosper together. The law books are littered with commentary from presidents and from jurists and from others talking about the threat to civil liberties, the threat to privacy in times of crisis, but also that both can be achieved when intelligent choices are made. When the public discourse is joined by policymakers, by advocates, by those in the private sector, and by the public, but we do have to make the intelligent choices. We have to build privacy protections into our technologies, into our policies, into our government. We must constrain the government, and this is somewhere where the left and right come together: a limited, focused government that constrains its power, that constrains its use of data, that constrains the collection of data about you makes for actually more effective programs as well as a less intrusive government.

The analogy I will leave you with is that I think data can be analogized to water. We need water to live. We need data to make this department and others run. But we – any homeowner who has had a leak knows that water gone wrong gets where it wants to go without your control. Data gone wrong – once data is in the house, it's going to want to flow, so we need the checks and balances, we need the rules, we need the regulations, we need the smart thinking that constrains the use of that data. And also I would say, as Jim made the excellent analogy to Amazon and to other online purchasers, that there is a vast difference between the use of your data in the private sector when you have given it to that company to provide you a service, whether it's buying a book or buying CD online, versus the provision of data to the government. The consequences for the misuses of data in the government are much higher and we should be that much more concerned.

Thank you.

MR. CROWLEY: Well, thank you very much.

I know everyone has comments – additional comments they want to make, so let me start back from left to right here. I mean, everyone says we are just starting; everyone says we got to serve both of these interests. We have had some experience already and it hasn't gone well for one reason or another. In addition to whatever follow-up comments, what are the lessons learned from TIA, CAPPS II, Jet Blue, because whether it's in the construction or the presentation clearly there is work to be done here to get it to a point that either the Congress or the American people have trust in what we are doing.

Jim?

MR. DEMPSEY: There may be some overarching themes, although when you scratch each of those they do display some differences. I think that TIA – John Poindexter's Total Information Awareness program really suffered, I think, from the hype factor. I think that if you had – if Poindexter had said, "This is a research program and I am not sure whether it will work." Remember, Thomas Edison, when he was looking for what would make the filament for the light bulb, tried like a thousand different kinds of things and they all failed until he figured it out and people said, "Well, gosh. Those were failed experiments. You did a thousand failed experiments." And he said, "No, no. They were all successful. I now know what doesn't work." And yet I think that some of the experiments that Poindexter was doing the outcome was suppose to be yes it works and they weren't true experiments because he was saying – at the same time he was saying we are doing research, he was saying I have the answer, and that's not research. And so he oversold and this – again, had this notion that there is this ocean of data and you can somehow find the bad guys there, and that's where we should put our resources and priority.

In terms of CAPPS, I think that CAPPS II suffered from a mission creep syndrome, which is a different kind of problem, I think, although I also do think in retrospect that there was some vendor hype going on in CAPPS. It turns out my conclusion is that CAPPS I is not so bad.

The whole rhetoric for about two years was CAPPS I is broken. The bad guys can game the rules, et cetera. It's not flexible. I think that I've now concluded that that was wrong. I've concluded that CAPPS I is pretty good. I also think we need to use the watch list (of flying?) passengers, but I think that CAPPS now – but anyhow, so people said, "CAPPS I is broken; therefore, we need to draw all this information and do some kind of black box predictive analysis," and again they were back into that. Outside of the – CAPPS I uses the data that is largely associated with your travel, and I think there is some validity – I think there is some proven validity there. That's one that I think has been proven; that if you look at some information about a person's travel plans, you can

then make a security risk prediction about who needs closer screening. CAPPS I flagged – was it seven or nine?

MR. CROWLEY: Nine.

MR. DEMPSEY: – nine of the 19 9/11 hijackers. That's pretty good actually. For all this predictive capability – I mean, in the marketing field, gosh, if you get one out of a thousand you are doing great. They got 9 out of 19. But then people started saying, "Oh, but in addition to catching terror" – with CAPPS II – "In addition to catching terrorists, we can catch illegal aliens or we can catch murders who aren't a threat to civil aviation, and we can keep the data for a long period of time because we are not really going to keep that guys off planes, but we are going to follow them as they travel," and it was this sort of, gee-that-would-be-a-neat-idea sort of phenomenon that happens. And finally more and more got added onto it that it just collapsed of its own weight. Now the government is trying to recoup with Secure Flight, which I think he has promise.

So I just think that people – they fail partly because certainly privacy wasn't taken into account and Poindexter made the mistake of saying, "I will design the technology. I will let somebody else worry about the policy." And the fundamental principle of technology design is that you have to build the policies in at the design phase. If you try to add the policies on afterwards, it's too late. Then I could talk more about some of the ways in which there are polices in which your security goal and your privacy or accountability goal are served by the very same technology.

So let me hold – let me tease you with that, but –

MS. KELLY: Well, I think P. J. actually set it up entirely, which it is both construction and presentation where privacy needs to be both articulated and also really truly felt and held by the program people, by the managers, sp I am not even going to be redundant and talk more about that.

Focusing on the technology – and that is I think really where the exciting possibilities, but also challenges exist for government and the private sector. Again, I come at it from my dot-com days, which obviously didn't work out too well or I would be not working right now. But we can get too caught up in the hype that the technology will be our savior; it will solve all these things. But I also that we can get caught up in the fear, which is "Oh, no. Biometrics scary. Don't want to have my picture taken at the airport;" those sorts of things.

You already have two biometrics on your driver's licenses most of you today. You have a photograph and you have a signature. Those are biometrics. The difference, of course, in a very real one is that a digitally captured and enabled one will be stored somewhere and so that is a very, very real difference. And we need to constrain, again, the collection and the use in ways that go back what Jim was saying: limit the mission and focus the mission of these programs on very clearly articulable (ph) and publicly agree-to goals, and I think the protection of our folks as they travel and move about the

countries is certainly an incredibly prominent and worthwhile one. So we should not, I think, fall into the knee-jerk, "Oh, it's great," or "Oh, it's terrible," reaction to any technology, but really have a conversation about does it do what it says it's suppose to do and do we want it to do that? And that is exactly right: you need to build in the privacy principles at the foundation.

Folks who say that, "Oh, I am going to worry about that later," or "That's somebody else's job," – there is a great debate on– let me just digress a little bit. There is a great debate right now in Congress about the role of the privacy officer and whether there should be more at other agencies and that sort of thing. I was talking to a very senior leader at another agency who said, you know, "We don't want a privacy officer." And of course I took great umbrage at this and he said, "We want every employee to think that privacy is their job." And that's very – I mean, I have to say that it's very compelling argument. I don't think it dismisses the role of a privacy officer because you need a senior level champion, someone who has got direct accountability to Congress, to the public, to the secretary, but you never want to have it cordoned off and (siloed?) off into one area where – oh, let's just check the mark. You know, we've got to send it to those privacy people like you send it to legal in the corporate America. You do want it to be fundamentally felt by every employee in you organization that part of their job is respecting privacy of their client, customer, citizen, whomever they are dealing with.

MR. CROWLEY: General?

GEN. CLARK: Well, several issues here. I guess it start with asking yourself what kind of society do you want to live in? I didn't like it after 9/11 when we had so many of our troops deployed in the airports. I thought it was a misuse of the troops. I didn't think it did much for our security, frankly. And I always like it better when I am not surround by a lot of police and uniformed officers and cars and so forth. So it's always a chilling thing you will – for years I was chilled when I drove down 110 past the pentagon and I passed the police cars that were pulled off, the Humvee with the soldier behind the 50 caliber machine gun on the roof and so forth, and I'd think, is that the kind of society you want to live in? If you don't want to live in that kind of society in which people are anonymous and potentially threatening, then you want to live in a society in which we have more awareness of each other, who we are, and maybe even where we're going – what our drives are.

Obviously, you can't get there totally. There was a Tom Cruise movie a few years ago that many of you probably saw where he arrests people before they can commit the crime. This is total information awareness. And I don't know if John Poindexter thought he could get that far, but it is the sort of Holy Grail of the information and data business that somehow through a pattern and sequence of activities you could create – you can see where forces are converging. So if you just spin out your imagination with the technology: you know that somebody on the watch list is loose, you have an alert that he has a credit card. Now you have an alert that he's bought gasoline at a certain station in Colorado. You know how much he has bought. You get the trigger 20 seconds after he's put his card in. You go through your voluminous sources and find out who owns

this store. If there is a video camera, now you've got a picture and you're able to roll back the data that the camera has recorded and take the guy's picture and confirm it's him. Now you have near-real-time location. I mean it's – you know, the next thing you're waiting for is you're tracking all cell phone calls in that cellular area. You then can sift through all the calls, find out who you don't know, and there is one unidentified number there from a cell phone that shouldn't be there that somehow has gotten logged on the net and you now are following as it moves from cell zone to cell zone and you intercept it. I mean that's the sort of total information awareness dream play.

I don't know if it would ever work or not, but I do know this: that it's – as the threat is out there in American society, it's a question how do we want to live? To me, it's better to move in the direction of greater use of data with appropriate safeguards than it is to try to block the consideration of the use of data. It is more efficient. It is more effective and that data is there anyway. So the question is, without trying to get into the Tom Cruise movie, how do you protect yourself as you are moving carefully step by step into a world?

When I was running in – last year in New Hampshire, the *Concord Monitor* editorial board – a woman said to me despairingly after an hour of interrogation. She said, "How am I ever going to raise my children in a society where they are not safe?" And it was like – you know, she was just so frustrated by this. There is an atmosphere of fear out there and maybe as we don't raise the terrorist alert level so much, the level of fear will go down, but it was high in 2004 and it causes perturbations in a lot of other things, so we don't want that level of fear. So this kind of use of data is one way to go at it.

So here are some of my rules on how it should be approached. First of all, we have to separate elements of data. People that wiretap shouldn't be collecting credit card information. People that have credit card information on background shouldn't be collecting transactional data. That's pretty much in place right now, so there are certain laws where they can't. Secondly, you have to encrypt data. There is plenty of encryption technology out there and it's not very expensive and it's NSA-approved and it should be mandatory in the data business. And third, you should be reporting to consumers on the data that's being collected and what the uses of this may be and you should be required to go back and ask them for permission to use data in certain other ways. Fourth, there should be a challenge process established like where you can go back and investigate your credit report. You would like to know what data is out there; there should be a mechanism for that. Fifth – I think I'm on five now – that we need to have a series of echelon of industry associations and maybe someone with oversight with some enforcement capability.

We don't know where the data industry is going. They talk amongst themselves. They all buy and sell data back and forth with each other. There is no reason why this can't be recognized in some way and they become like a self-regulatory – regulatory organization like the National Association of Security Dealers, for example.

And finally, the best standard of all is the standard that's in the due process laws. It's the way we always approached the issues in the military. The greater the consequence of the use of data or the violation of privacy or personal intrusion, depending on how you parse it, then the greater should be the due process protections for the individual. So if you are standing in line to get into a bar at night and somebody says you can't come in, then that's not very consequential and there is not much you can do to challenge it. If you are on a watch list and you are barred from flights and searched every time you get on a flight because of your name, then there needs to be – that's pretty significant and there needs to be a formal, clear, easily articulated and understood due process challenge to that and so on as we work through it. But I think if we have rules like this that are commonsense rules, it's possible to do more with data, and doing more with data makes it possible to live in a freer society that still protects privacy.

MR. CROWLEY: Thank you, General.

Robert, you get the last word before we open up for questions.

MR. O'HARROW: I am going to relate some thoughts that correspond to some of the very interesting ideas that they have shared, but I'll let you connect the dots among them.

First of all, I have been striving with some success to redefine the discussion as about autonomy, not about privacy; not that we should discard privacy as a word altogether, but I think of it more of as a tofu word so that we can all apply whatever flavor on it that we want; whereas autonomy, in my mind, is about the relationship of the individuals to institutions, whether it's me to Axiom or me to the DHS and the government in general or me to American Express.

And the idea is that those institutions have a hell of a lot more information about me than I have about them. They are spending a lot of money trying to figure out how to apply that to shape my behavior in some way, in many cases, and I don't know what they are doing. We're at the very beginning of that in a sense, although of course this has always gone on, but with the data revolution, it's much more possible for institutions to define me, to profile me for risk, to decide that I am the 20 – among the 20 percent most profitable customers or the 80 that they shouldn't care about. And so its really autonomy: it's this notion of that at some level we have a right to be let alone that is fundamentally at the core here, so that's one thing.

Two, Jim Dempsey talks about the hype of the predictive analysis. There is no question there is a lot of hype out there and that a lot of it – the claims for this stuff exceeds the reality, but there is also no question that they can do a hell of a lot more than they did 10 years ago even, and that the power to connect the dots in a sea of data is growing rather rapidly. We've even made a policy at the Justice Department and FBI that we are as a country, they are as a department and as an agency, going to be predictive and proactive. That's a stated goal by the Attorney General John Ashcraft and Mueller. Companies like i2, which was acquired by another company called Choice Point – there

mission is to look into data and using a variety of mathematical and data-mining techniques and such is to find links among people.

I, too, could find the links all of us – among all of us, how we are tied together, and then could create a nice, large, interactive map and it could show the links among us via our classmates in college, the houses that we have owned, our neighbors, the phone numbers we have used. That's the type of intelligence that is being used routinely now on behalf of the government. The government's outsourcing intelligence and the security imperatives to these private companies. And of course we look back to go ask Choice Point how they are doing that and they will say, "Well, you'll have to ask the government." You go to ask the government; they say "Well, can't talk about it because it's security sensitive." That's going to be a reality for the rest of the lives notwithstanding the hype.

And by the way, when there is hype it means that they can't do what they are always claiming to do, but the users don't always know that and as a consequence they are using tools that are flawed by definition, not – that doesn't mean they are bad. They are flawed by definition, that rely on data that's flawed by definition, which means that they're relying on things that are deeply flawed and they don't know it, which means they're going to make a mistake as they did in the case out in Oregon with a lawyer who was converted to Islam and everybody knows that story and if you don't, we can talk about it later. But his house was turned upside-down, hundreds of photographs, his records were taken, he was thrown into jail and then at the end the FBI apologized for the mistake that it made.

I want to very, very gently take issue with a couple of things that Nuala had said about DHS, and more broadly I think we have to remember something about these discussions going forward, and I am speaking as a reporter here so discount it however you want. I have found that I can't always believe what my government tells me as reporter. I have many instances of that. They are in my files. I have got the papers. I have got direct contradictions between things that my government told me and things that they were actually doing, and it happens over and over and over again.

Now, in 2003 and 2004, I noticed there seemed to be a pattern. It seemed like a lot of things that were said were for public affairs impact or for public relations impact and, gee whiz, when you go look at the contracts there – where you have outside contractors that are helping on the national security apparatus there are paragraphs – I got a new one last night – that say how to create a favorable public image. You may remember a 90-day plan by one of the homeland security agencies in September; a 90-day plan for presenting – you know, reinforcing the idea that we're safer than we were on September 10th, 2001. Arguably, we are. No question, et cetera. But there was a plan inside her department – DHS – to drive that home through a public affairs apparatus and at some level you have to wonder, well, how much of this is fact and how much of this is a favorable kind of spin or something else?

Why does that matter? Well, let's go to one issue; for example, CAPPS. Jim Dempsey talked about CAPPS II. Does everybody know a CAPPS is – CAPPS II? It's the system that was being created at some cost – the last I saw it was about $100 million, but it's probably much higher than that now since my numbers were out of date. They spent a lot of money and they relied on companies like LexisNexis; they relied on Axiom, Lockheed Martin, and then some other very high-tech, very data savvy companies to create a system that would create a profile or a model of every passenger and their rootedness in the community, so it was going to look at data and define were you really a human being that really existed in a particular place and time and do you exist in that place in the way that your cohort does. In other words, do you have a dog, a car; do you own a house? If you are 44, are you still renting in a $600 apartment with four other guys who happen to be Muslim or are you living in a house with the kind of car that everybody else drives? That was actually going to be the model and, believe it or not, in some ways, it wasn't inherently bad. I actually believe that we have to have some sort of aviation screening system. It's foolish not to take advantage of information technology to know who is on that plane next you and use that in a very narrow way.

Now, in writing about CAPPS as a reporter – to remind you where I am coming from – I spoke to very senior people in the government who said over and over again – they made promises to me in the sense that I was going to convey them to you that this was not going to be used as an all-purpose law enforcement checkpoint. This was going to be used to screen people to keep terrorists who would kill themselves and thousands of others along with them off of airplanes. Over and over and over as they are (spinning?) this, and I am dogging this thing. I made it – you know, it was kind of my assignment and I worked very hard at it and I have reported that, and I believe the promises and I still do by the way. I know the people I was talking with, including Michael Jackson, were telling me straight up and they were working hard and I knew that because I never just believe what someone tells me, I check it out, and I checked him out. I checked out Jim Loy. I heard about meetings they had with privacy advocates. I knew about meetings they had with companies like Axiom, and they were really working hard to try to have a system that could be used narrowly and for the common (will?).

In the summer of '03 – July '03 – I try to make sure I get the dates right, there was a Federal register notice where Homeland Security said, "We are going to use this to stop violent criminals who are wanted and immigrants who are overstaying their visas or whether – or whatever, as well as domestic terrorists, on top of the terrorists from abroad." Suddenly, there was this huge expansion of the mission, which had practical impacts. Of course we want to stop violent criminals; everybody wants that. We do not want rapists and murderers traveling on the airplanes and maybe going to commit another crime.

But there was also another issue that was very important: by expanding the mission, the DH folks didn't realize this at the time, but they were sealing – in my estimation, they were dooming the program, which we needed, right? They were dooming it because of the backlash that was going to occur on the Hill and among people because a lot of people were going to be freak about the expansion; it was going to be a

real tumultuous issue, which was exactly what happened by the way. But when that was announced, it was announced with great sincerity, "This is not an expansion. This is not an expansion at all," and I just found that disingenuous and it's the kind of message that you have to take with a grain of salt. They are telling you this is not an expansion, when of course it was an expansion and of course when they decided to end CAPPS and create Secure Flight they themselves said that was an expansion that was not a wise one and didn't suit the interest of the American people. So the bottom-line message is we have to be very, very careful about how we debate this stuff. We have to have true openness in the debate and we can't just go one platitudes or PR spin.

One last thing, the issue of FOIA that was brought up. And in that spirit, don't let anybody kid you, the FOIA system is a travesty right now. It's a travesty in part because the attorney general of the United States wrote a letter, which I have – I'm happy to share it with anybody, it's out there – that said make whatever efforts you can, in effect, to not share freedom of information labeled documents; you know, limit that. Hinder that process, in effect. I'm sorry I can't quote from it, but the spirit – I believe I'm conveying the spirit of that letter. And the fact is if anybody in this room – and I'm sure there are some reporters here who have tried to use FOIA to find out what our homeland security officials are doing, they'll probably concur that it's not an open process. We don't have access to information that should be open, and that that's something that needs to be fixed.

MR. CROWLEY: Okay, a fair amount of grist for the audience. You know, by all means, as Theo comes around, please identify yourself, and let's keep the questions brief so that we can continue the discussion. Questions? Let's start over there.

Q: Thank you for organizing this. My name is Ingrid Drake. I'm with Pacifica Radio Network. And my question is to you, Ms. O'Connor Kelly. I've been following a case up in British Columbia of a contract between Maximus, which is a U.S.-based firm in Virginia and the British Columbian government in terms of information technology with their population's health information. And I want to know what is currently in place to prohibit the Department of Homeland Security from accessing information from U.S.-based firms about citizens of other countries?

MS. KELLY: Let me make sure I've got your question clear. You're not asking about health information, you're asking about citizens of other countries, generally?

Q: Any of the (off mike).

MS. KELLY: Okay. I'm not at all familiar with the Maximus-British Columbia case, but the use of information about international persons coming into the country is something that our office has worked on very seriously, very significantly, from the earliest days of the office. But let me just give you the history really quickly, the Department of Homeland Security opened formally on April 1st of 2003, I believe, and I was there on April 16th, so that's how early in the process we were part of it. In fact, currently we have a number of international agreements – there are a number of

international legal agreements between our government and other governments for the passage or the prevention of passage of international travel information. For example, one that you may be very familiar with is the use of passenger name records, PNR data, that come into the country with accompanying international visitors. We have put some very serious constraints and limitations on the types of data.

Just to go back to your question though, particularly about health information, obviously the number one constraint in the United States is HIPPA, the Health Information Portability Privacy Act, which limits the use of your health information in any way other than the way in which you expect it to be used by your doctor and unfortunately by your insurance company and others in the healthcare system. And obviously now you're getting, as you get in the banking world, a lot of notices when you go to the doctor that say here's how my data will and will not be used. We have not to my knowledge at Homeland, in the two years I've been there, had any scenario in which we have used health information about citizens.

We do collect personal information, obviously, on travelers coming into the country. We have within Homeland, you should all know, not the CIA and NSA and FBI, which a lot of people think are in Homeland Security, outside of the beltway at least, but we do have Customs. We do have immigrations – all the former Immigration Service folks, we do have the Transportation Security Administration. So all of those parts of Homeland will meet at the border visitors to this country, and like when you go to any other country, they will access your passport, your information, your travel documents to know whether you are on a legitimate visa and those sorts of things. So, yes, the Department of Homeland Security does collect personal information about visitors to this country again for the purposes of immigration, for customs enforcement, for border enforcement, and for travel.

Q: (Off mike) allows you all to (gather?) any information you want (off mike) so there's nothing (off mike).

MR. DEMPSEY: You know, okay, wait a second. The first question to ask is what prohibits the U.S. government from acquiring data about U.S. citizens, okay? Leave aside the Canadians because I think it's the same. The government has the authority to compel the production – to force the production of data through a court order, a subpoena, a national security letter, et cetera. By and large, what we're talking about here is the government buying the data where the seller voluntarily sells it or the government actually subscribes to it – they don't acquire ownership of it, they acquire a subscription right. There is nothing – nothing? – there is very little prohibiting the U.S. government from buying data about Americans and *a fortiori* there's very little U.S. law prohibiting the U.S. government from buying data about Canadians. Now there may be a Canadian law that prohibits a Canadian company from shipping data on Canadians to the United States, although most privacy laws do have national security exceptions in other countries.

I mean, the European – we talk about that sort of great privacy laws in Europe. I say that a little cynically, but they have a national security exception. And I'm sure that whatever Canadian privacy law – PIPIDA – has a – what's the acronym in the law? It has a national security exception. Now, whether that covers the sale of Canadian – it certainly allows – Canadian companies, I have very little doubt, can provide data to the Canadian Mounties and to the Canadian Intelligence Service. They may or may not be able to sell their data to the U.S. government. But there's no U.S. law that prohibits the U.S. government from buying data from a willing seller overseas, just as there is no law that prohibits the U.S. government from buying data from a willing seller in the United States.

Q: (Unintelligible) and thank you for setting this up. My name is Eric Massy (ph) and I'm a retired naval officer and a candidate for Congress. My question deals with what I perceive to be a fundamental disconnect between technology and our enemies. There's an awful lot of conversation and an awful lot of effort about gathering data in a highly technological world, and yet it strikes me that the bases of our fundamental enemies exist outside of that technology. And so inside of the argument (and purview?) in Homeland Security and in reporters and in the national security apparatus, how do we apply these tools against a training camp where no one has credit cards, cell phones, or any of those other high technological issues that we have to focus us?

MR. CROWLEY: I'm not sure I accept the premise of your question, but generally, you know, these are becoming more sophisticated people. And as the 9/11 Commission pointed out, when – you know, if you're going to attack the United States, you're going to travel. When you travel, you're going to expose yourself to certain things that put you open to detection with – you know, so, yes, in Kandahar there's a limited American Express presence so far, but I'm not sure I accept the premise that when you come to our world with the intent of attacking it that you're necessarily going to be able to continue to operate under the radar with that.

MR. O'HARROW: There is kind of an interesting point there. We need to use information technology to look for signatures at some level. The NSA devotes a lot of time and energy trying to do that, signals intelligence – you and the general know a lot more about that then I do. The challenge here is using technology when they intercept – we don't – you're right about if they're in the mountains of Kandahar it's going to be really hard because they're not leaving that signature. They're going to intersect with our systems when they fly, when they travel, when they set up a bank account here.

The challenge is discerning these folks from graduate students, right? Because we have money laundering systems in place that are very, very good and getting a lot better. These are the use of artificial intelligence and neural networking and all these fancy things that establish a baseline profile of an individual and a cohort and then look for deviations. Well, a lot of that's for money laundering when they're moving lots of money and they're trying to hide it and wash it, but how do you detect when someone is a terrorist because they're paying a low rent and they're not eating very much food and

they don't spend a lot of money, which is what terrorists often do. So the point is, that you've raised, the bottom line is it's a real challenge.

MR. CROWLEY: Let's go there and then go towards the back.

Q: Hi. It's Andrew Noyes with *Communications Daily*. I just had a question for all of the panelists, if you could speak for a few minutes about specifically the state of cybersecurity, the challenges that we face, and where we're headed in that particular arena?

MS. KELLY: (Off mike.)

MR. DEMPSEY: I'm very sorry, I was – could you repeat the question?

Q: It is the state of cyber-security. Obviously, the – part of the challenge here, as we know from Choice Point and others who have had dilemmas here with the disclosure of information how – you know –

MR. DEMPSEY: Yeah.

Q: How do you protect what we're gathering on our behalf?

MR. DEMPSEY: Well, one of the fair information principles is security. The principle is that a person who holds personally identifiable information has an obligation to protective security. I think we are inching forward towards some general regulatory obligation on behalf of people holding personally identifiable information. Obviously in the healthcare industry there is such an obligation as a result of HIPPA. In the financial sector there is such an obligation as a result of Gramm-Leach-Bliley – Financial Services Modernization Act. If you look at the regulations under those though, you will see how process oriented they are as opposed to substance oriented.

The issue in the computer security field generally and the vulnerability is huge on the critical infrastructure side: power, energy, transportation, just the flow of money, leaving aside privacy. Huge, huge vulnerabilities still not resolved. The problem is we have no standard of care. We have no definition of what is good-enough computer security. It's a little bit though like what General Clark was referring to in thinking about the evolution of industries.

It is really remarkable that I – you probably all seen those charts or reports about how long did it take 50 percent of the American population to get radio? You know, it was something like 50 years. How long did it take 50 percent of the American population to get telephones? It was 70 years or – how long did it take 50 percent of the American population to get the internet? It was like, 10 years. So we've had this industry that has grown, this information and communications technology sector that has grown at a huge, huge rate, and now people are saying, okay, what's the regulatory framework? Great, we've got this, now what are the responsibilities? And in a way,

security is the flip side of privacy and we're just getting up to the edge there from a civil liberties standpoint, from a sort of open networks innovation standpoint, the last thing I want to see is the government dictating specific security practices.

Among other things, I think the surveillance objectives would end up always trumping the security objectives, and we'd end up building in vulnerabilities at the demand of the government, but I think we are edging to a regulatory regime for this. I think it will be a mix of self-regulation, industry standards, and some governmental oversight.

(Cross talk.)

MS. KELLY: It's just incredibly important, I think: the issue of cyber-security in relation to privacy. And you see it in the data spillage issues we've had in over the last six or eight weeks in the private sector, and it obviously greatly affects government databases as well. I liken it to the industrial revolution. I think Bob described this as the data revolution, and that's exactly right. You had environmental spills. You had environmental challenges. You had impact on the world from the industrial revolution. So we are having impact on our lives from the cyber-security challenges, the data revolution. We do not – we have not kept up with our need to act as stewards for the data if we are going to collect vast amounts of data, and that's why we call these – often I hear them called "data Valdez." They are data spillages which have privacy implications for each one of us whose data may be held by the private sector or the government.

And so as we got into the environmental law and environmental compliance in the corporate sector 20 years ago, now I think we are in an age of privacy compliance, of data quality, data accuracy, data protection for our institutions, whether they be private sector or public sector. And I think that Jim is exactly right, that we perhaps have not kept up with either our laws or our self-regulation in a way that thinks about the seriousness.

I mean, one analogy I used to use about data is that it's like blood. I mean, we need to treat data with the kid gloves that we would want our personal information treated by in the private sector or in the government. And so we need to move forward with whether it's ruled, and I agree with about – with Jim about not setting up rules in the government for the private sector on security, but a standard of care at least for personal data held by any institution. And we can look to laws that exist already and whether there are shortcomings that may need to be addressed.

MR. CLARK: You know, I think one of the great secrets of business is how much they lose by not securing elements of their information architecture. They normally won't disclose this. I mean, it's happened that you've found out this data was lost by Choice Point because they had to, but other companies who don't secure data and have it ripped off by an employee or have fraud committed by employees by use of unsecured data internally, they seldom publish that information. It's bad for the company's reputation. It doesn't develop business confidence. And so I think that we do

need government standards. I think that in – throughout the homeland security area, one of the things that's most missing is a better grip on what standards are.

For business – except in the case of protecting against losses, security measures that businesses take are costs and no businessman likes to add to the bottom line cost unnecessarily because it takes away from profit. And if the competitors aren't doing it, it puts you at a disadvantage. So when you walk into an office building in New York and you get stopped, and you go through security, remember that's not adding anything to the profit of any company in that building; that's just a cost that they're paying. It's the cost of doing business.

The thing is, there are a lot of industries in which – and maybe cyber-security is one, in which the costs aren't – it's not clear what needs to be done in which the public cost is greater than the sum of the private costs for not taking action. Another one of these industries in addition to cyber-security might be the chemical industry. And what people are looking for in these industries, they're looking for some guidance as to what should be done. What's a reasonable standard of protection? And I think that as we get into this area, that is an obligation the government should take. Just as the government oversees and does regulate certain other functions in America that have to do with health and safety for American consumers, the use of data and how that data is stored and transported so forth should be properly a matter of public concern, not just a matter of private profitability.

MR. O'HARROW: Just a short thought that Nuala made, I thought, a very good analogy to the industrial revolution and pollution and this idea that businesses providing us very, very good services back in the '50s in the heartland – in Gary, Indiana, and in Ohio and Pittsburgh – were not absorbing the full cost of doing business, which is accounting for the pollution that they were creating. That had a lot of side or external effects on people: respiratory diseases, you couldn't see the sunlight in the middle of the day, et cetera, et cetera. And the good news here, and this is the rosy Indiana optimist speaking, is that we're at an early enough stage here that I'm very confident that the information industry is going to figure out how to use the technology that they're very good at using to provide the security and to deal with some of these issues – these external issues like the epidemic, I guess, of identity theft. We certainly know it's widespread – so that they're going to use the technology just as the industrial companies did to clean up the air, to clean up the data insecurity and the security vulnerabilities, so I think we're going to see that. It may take a while and it's certainly going to take some pressure just as it took pressure in the environmental world and the meat-packing world, et cetera.

MR. CROWLEY: I'll take this gentleman right here at the aisle. Well, wait for the microphone.

Q: My name is John Shell (ph) and I represent Hampshire Research, which is a public interest data analysis firm. At the heart of the issue for both security and privacy is the intentions of the individual. If we're going to integrate data, we need to know who

we're talking about, who we're going to protect, the propagation of data of an individual, and we need to know who we're talking about.

For any of the panelists, what is the advisability and your recommendations for an approach to a dispositive electronic ID for individuals? Should this be under the control of Big Brother or the Marlboro Man? Should we create such an electronic identity? How should it be created and controlled?

MR. CROWLEY: It's a great question. Let me just broaden it slightly because it was going to be my last question to the panel. You know, talk about that question and then are we focused on the right thing or the wrong thing? There's an argument going on about the credential, but is it really the credential or is it the system behind the credential, whether it's a smart driver's license or a national ID?

MR. O'HARROW: I just want – I'll be very quick. I really like the idea in theory of a fingerprint or some sort of biometric because it would eliminate so many problems. It would wipe out much of identity theft, and it would ease things. It would even add more convenience in many ways. The problem that we're going to have to confront are the problems that everybody on the panel has talked about which is, how do we ensure that that doesn't become a source of secret influence? In other words, enhancing the data revolution and enhancing the imbalances that Dempsey talked about and the sorts of things that Nuala was mentioning or using it narrowly with great restrictions and consequences for the misuse in order to do what – address an issue that the general talked about, which is the key issue after 9/11, I believe, which is identity. How do you authenticate if someone is who they claim to be?

The problem is, of course, if you adopt a fingerprint and a universal biometric of some sort, then you use it to link all these records and to create new information whether it's getting into a building or signing onto your cell phone or computer; the list goes on and on, getting groceries. Some grocery stories, by the way, did you know that you could charge now – in some pilot programs you can charge by giving your thumbprint, which is really fascinating. How do we ensure that when you do that that it just doesn't get out of control? Because it fact if it were misused it would actually accelerate all the bad things while providing us with new conveniences, but that's the – to me, that's the key issue, I think. And it would be a great solution if we could figure it out.

MR. CLARK: I'm inclined not to favor a national ID card. I would like to find – I mean, that's my last – that would be the last, last, last, last alternative. Surely, there are other ways to keep us safe. And I just think that it's about autonomy, it's about privacy, it's about who we are, and there are other ways that are less emotional than that. This is a huge emotional issue for Americans who traditionally – you know, freedom is part of – being free in America is sort of being left alone by the government. It's what you say is autonomy. So, you know, I think that the obligation is on those who want to create a national ID card that there really isn't any other way to handle the complexities of modern society without it.

MS. KELLY: I agree very much with the two previous speakers. And I would also – I would say that I think the technology holds promise, but it also holds great concern and that the constraints need to be built in not only at the front end but at the back end. What if someone – somehow the file gets messed up and you've got somebody else's fingerprint associated with you. How do you get that fixed? It's hard enough to get your name corrected at the Social Security Administration or the DMV. We need to make sure we've got the front-end system and the back-end systems in place before such things are rolled out.

I will say, at Homeland, we have demonstrated there is a difference between the name based and the biometrics. The U.S.-Visit program has not only, to my knowledge, never prevented anyone from getting on an airplane incorrectly or not being able to pass through their lives, but has actually apprehended not only hundreds of visa violators and that sort of thing, but actually it is part of their mission, and they've apprehended many, many felons and people who – and wanted murderers and people from coming into this country. And so with greater accuracy they have been able to not interfere with the innocent traveler, but have been able to prevent the known or wanted person from coming into the country. So there has been great promise, but again, great controls were placed on that program before it ever was launched.

MR.CROWLEY: Just to follow up –

MR. : Just –

MR. CROWLEY: – for one second. Have you had a chance to examine the difference between what was in the intelligence reform bill in terms of a stronger driver's license and now what's being proposed as part of this real ID?

MS. KELLY: It's certainly something that my office is looking at. I can't say that I am the expert. I have already been quoted as very flippantly saying I'm not a fan of the national ID either. I do think it's also wise to at least look at the fact that we have a de facto ID with our driver's licenses and confront very practically the combination of our driver's license, our social security number, and the vast file that exists in the private sector and say what are the limitations, what are the constraints we want to place on those? We certainly want to be able to get ID to provide driving abilities for citizens in this country, and we want to provide those services at the state and local as well as the federal level, but how do we make sure that when we give our information to the government it is only used for the purpose that we provided it and no other?

And frankly – I think I'll take this moment to respond to something Bob said earlier. The way we do that is to watch our government very carefully and to be vigilant and to use the FOIA, which I will argue, at least at Homeland, is working extremely well with over 400 people working full time to respond to almost 200,000 requests last year. So we're doing a great job on FOIA. But also to look very carefully at the disclosures.

Bob may have talked to hundreds of people about CAPPS II, but I point you to the documents – the legal documents that were published on CAPPS II in December of 2002 and July of 2003. There were differences and they were very meaningful, and they were – in my opinion, they were limitations, but there also were (growth?). It's fine to have to listen to the promises, and I would agree with Bob. Look at what the words are on the paper. Look at what the law says because people may change. We have a new secretary at Homeland. We may have an – we have a new – we have a third director of now Secure Flight. We have to look at what our government promises because when that person leaves, all their promises leave with them. The law stays. So let's make sure the law says what we want it to say.

MR. CROWLEY: Jim?

MR. DEMPSEY: Just going back to the question, I'll say that I'm skeptical of the single identifier – single electronic identifier. I think we need different identifiers and different forms of authentication for different purposes. I worry that the single identifier becomes a vulnerability if it's compromised, so if everything is linked to a particular system or a particular ID, and I think the perfect example of that is a Social Security number, which has become a major point of vulnerability for identity theft.

I think the questioner – I assume is well aware of the distinction, but the distinction needs to be drawn at any discussion of ID between an identifier and an authenticator. The Social Security number is an identifier. An authenticator proves that you are who you claim to be. A biometric is an authenticator. You can use it as an identifier too, but it's an authenticator because it's you and only you. The trouble with the Social Security number is we confuse that, and we took an identifier and we use it as an authenticator, because when you call and people say, "What's your name? And for security purposes tell me what your Social Security number is," or "Tell me the last four digests of your Social Security number," they're assuming that your Social Security number is secret and that, therefore, if you have it you must be who you claim to be; and, of course, your social security number is widely available. And so that was a case of an identifier being used as an authenticator. I think we have to break that distinction, particularly with the Social Security number.

Whether the questioner was talking truly about an identifier or whether he was talking about an authenticator, I still think in the online context, as well as to some extent in the offline context, we need different identifiers and different authenticators for different purposes rather than a single one because, A, it's very complex, and, B, it introduces vulnerability.

MR. CROWLEY: I know everyone's frustrated because it's now 11:33. We promised we'd have you out the door at 11:30. And we knew coming in this was a very fascinating, important, complex, vast issue, and we would never satisfy it all in two hours. I think we're going to have to leave it there and apologies to those who've had their hands up and want to ask more questions. I think the panelists may stay here for a couple minutes, if you will.

Just a couple of quick things. Thanks to a variety of colleagues at the Center for American Progress, Reece Rushing and Raj Goyle in particular, for helping set up this wonderful panel. We have a couple of national security related programs coming up that we'll be talking about. On May 16th, a program on a unified national security budget and on May 12th we'll have a program on bio-security, public health, and the role of industry. But we will be coming back to these national security, homeland security issues on a regular basis.

We thank you for coming. We're adjourned. (Applause.)

(END)